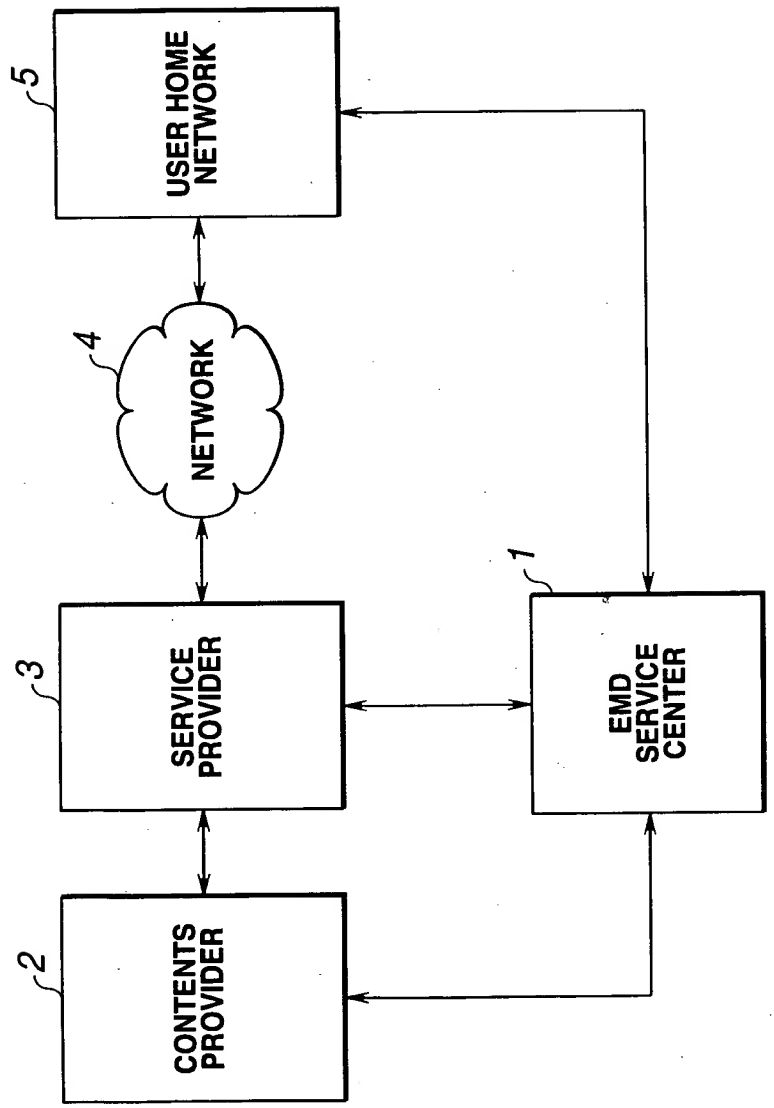
USER HOME NETWORK
5
NETWORK
4
SERVICE PROVIDER
3
EMD SERVICE CENTER
1
CONTENTS PROVIDER
2

FIG.1

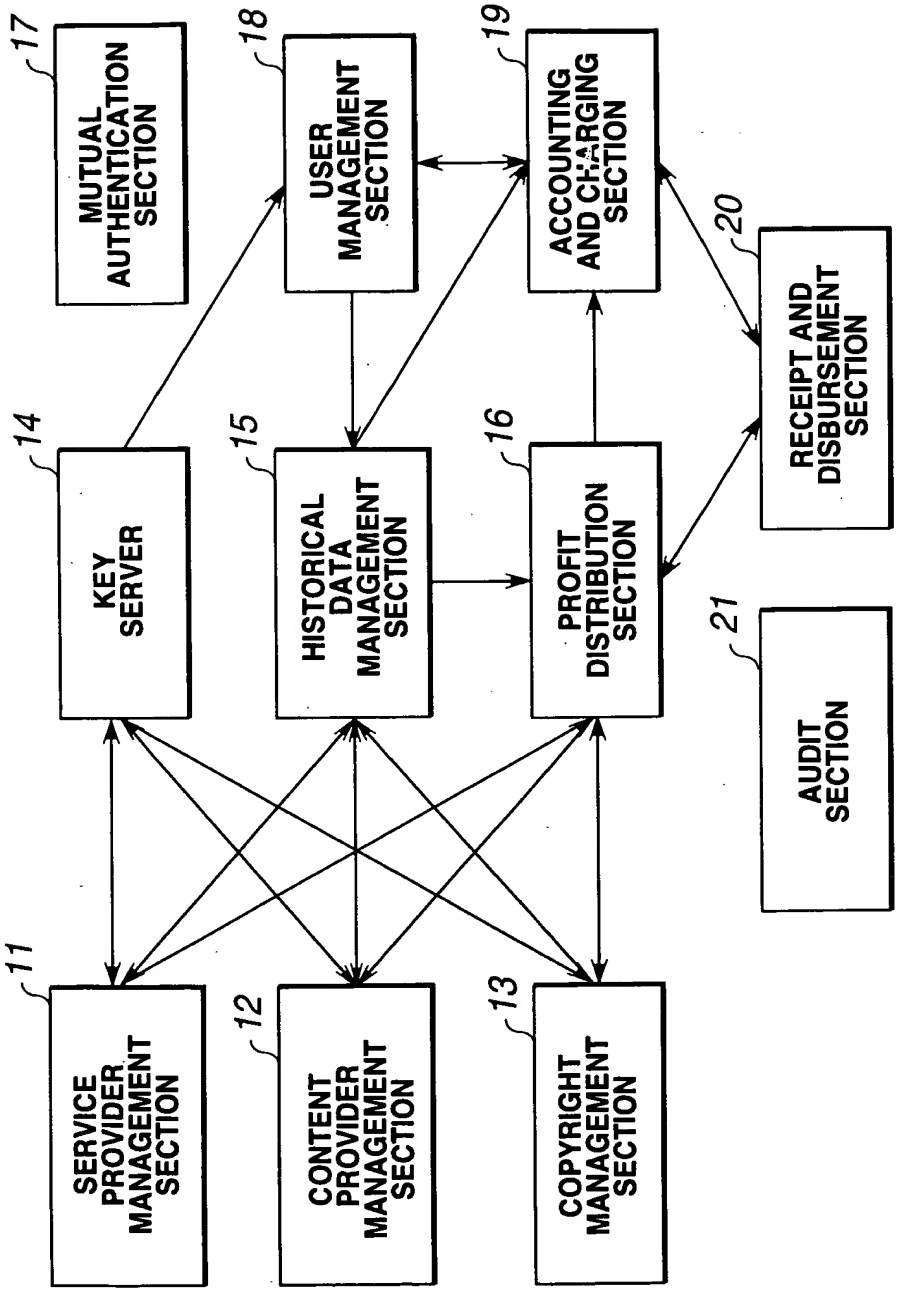
17
MUTUAL AUTHENTICATION SECTION
18
USER MANAGEMENT SECTION
19
ACCOUNTING AND CHARGING SECTION
20
RECEIPT AND DISBURSEMENT SECTION
14
KEY SERVER
15
HISTORICAL DATA MANAGEMENT SECTION
16
PROFIT DISTRIBUTION SECTION
21
AUDIT SECTION
11
SERVICE PROVIDER MANAGEMENT SECTION
12
CONTENT PROVIDER MANAGEMENT SECTION
13
COPYRIGHT MANAGEMENT SECTION

FIG.2

09/581583

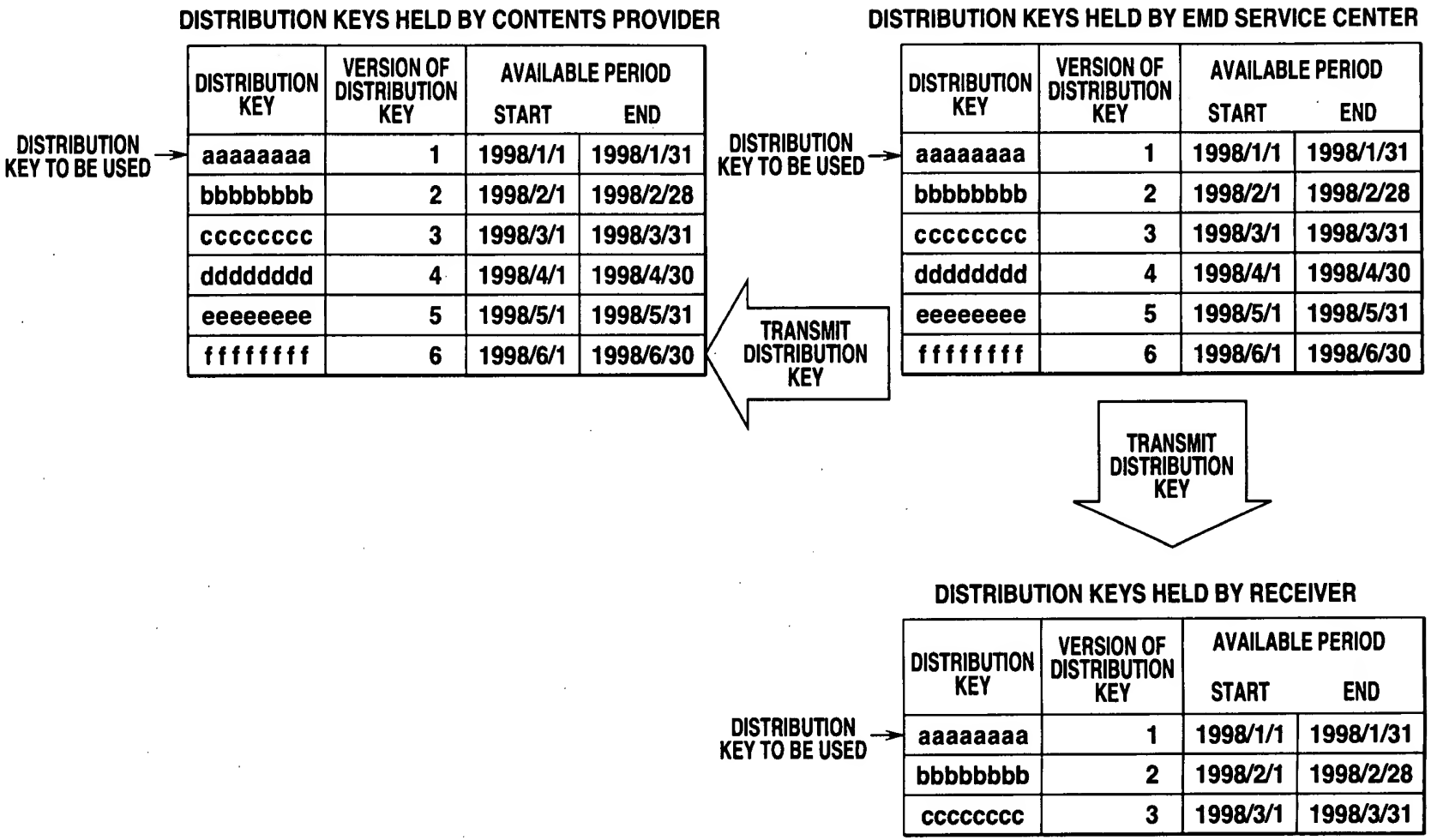

FIG.3

DISTRIBUTION KEYS HELD BY CONTENTS PROVIDER

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

DISTRIBUTION KEY TO BE USED →

TRANSMIT DISTRIBUTION KEY

DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31

DISTRIBUTION KEY TO BE USED →

TRANSMIT DISTRIBUTION KEY

DISTRIBUTION KEYS HELD BY RECEIVER

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30

DISTRIBUTION KEY TO BE USED →

FIG.4

DISTRIBUTION KEYS HELD BY CONTENTS PROVIDER

DISTRIBUTION KEY TO BE USED →

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

TRANSMIT DISTRIBUTION KEY

DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER

DISTRIBUTION KEY TO BE USED →

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
aaaaaaaa	1	1998/1/1	1998/1/31
bbbbbbbb	2	1998/2/1	1998/2/28
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31
ffffffff	6	1998/6/1	1998/6/30
gggggggg	7	1998/7/1	1998/7/31
hhhhhhhh	8	1998/8/1	1998/8/31

TRANSMIT DISTRIBUTION KEY

DISTRIBUTION KEYS HELD BY RECEIVER

DISTRIBUTION KEY TO BE USED →

DISTRIBUTION KEY	VERSION OF DISTRIBUTION KEY	AVAILABLE PERIOD START	AVAILABLE PERIOD END
cccccccc	3	1998/3/1	1998/3/31
dddddddd	4	1998/4/1	1998/4/30
eeeeeeee	5	1998/5/1	1998/5/31

FIG.5

09/581583

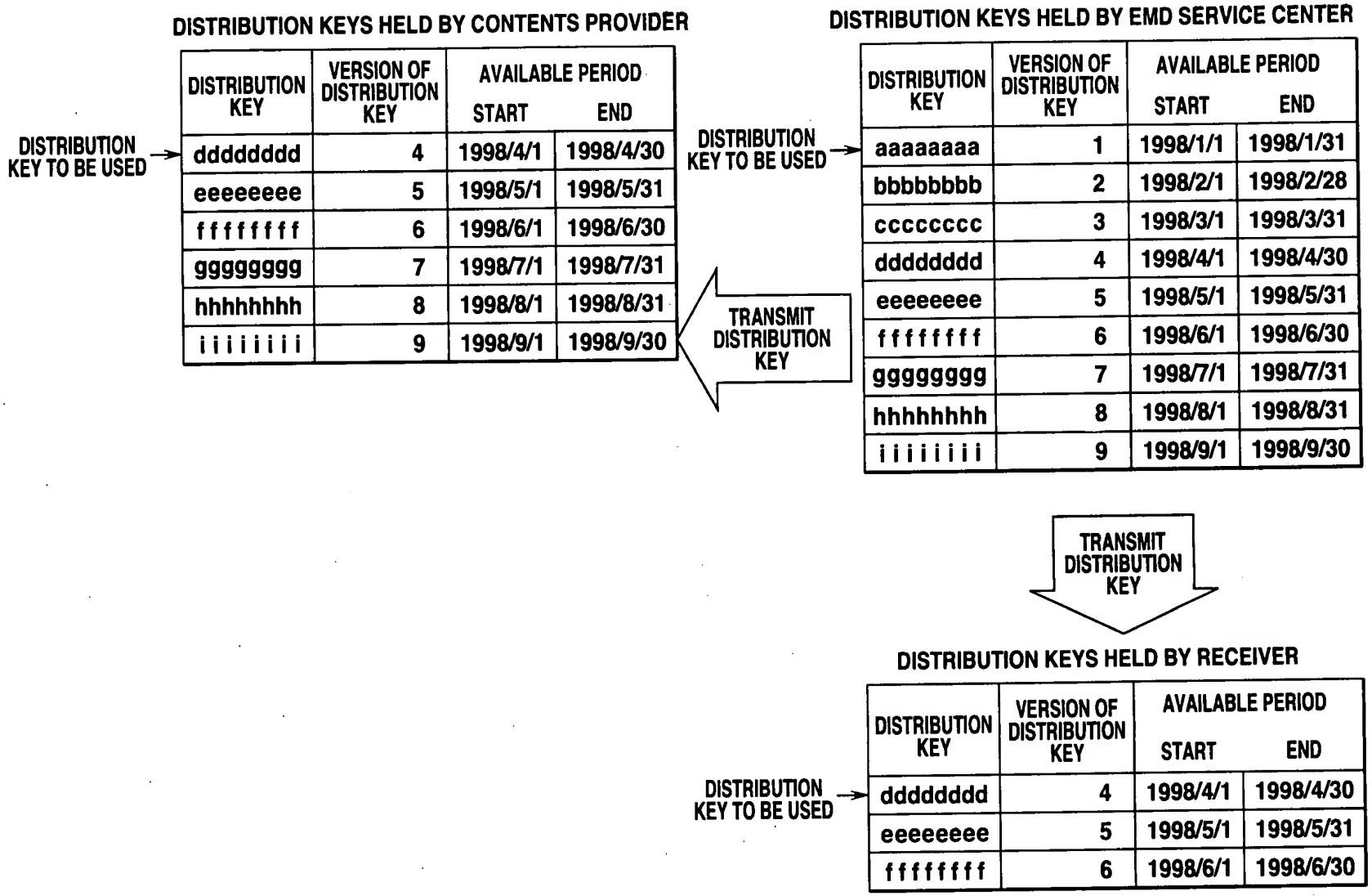
DISTRIBUTION KEYS HELD BY CONTENTS PROVIDER
DISTRIBUTION KEY
VERSION OF DISTRIBUTION KEY
AVAILABLE PERIOD
START
END
DISTRIBUTION KEY TO BE USED
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
TRANSMIT DISTRIBUTION KEY
DISTRIBUTION KEYS HELD BY EMD SERVICE CENTER
DISTRIBUTION KEY
VERSION OF DISTRIBUTION KEY
AVAILABLE PERIOD
START
END
DISTRIBUTION KEY TO BE USED
aaaaaaaa 1 1998/1/1 1998/1/31
bbbbbbbb 2 1998/2/1 1998/2/28
cccccccc 3 1998/3/1 1998/3/31
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30
gggggggg 7 1998/7/1 1998/7/31
hhhhhhhh 8 1998/8/1 1998/8/31
iiiiiiiii 9 1998/9/1 1998/9/30
TRANSMIT DISTRIBUTION KEY
DISTRIBUTION KEYS HELD BY RECEIVER
DISTRIBUTION KEY
VERSION OF DISTRIBUTION KEY
AVAILABLE PERIOD
START
END
DISTRIBUTION KEY TO BE USED
ddddddd 4 1998/4/1 1998/4/30
eeeeeeee 5 1998/5/1 1998/5/31
ffffffff 6 1998/6/1 1998/6/30

FIG.6

ID	SETTLEMENT PROCESSING	REGISTRATION	CONNECTION WITH EMD SERVICE CENTER
0000000000000001h	POSSIBLE	POSSIBLE	POSSIBLE
0000000000000002h	POSSIBLE	POSSIBLE	IMPOSSIBLE
0000000000000003h	POSSIBLE	IMPOSSIBLE	POSSIBLE
0000000000000004h	POSSIBLE	IMPOSSIBLE	IMPOSSIBLE
0000000000000005h	IMPOSSIBLE	POSSIBLE	POSSIBLE
0000000000000006h	IMPOSSIBLE	POSSIBLE	IMPOSSIBLE
0000000000000007h	IMPOSSIBLE	IMPOSSIBLE	POSSIBLE
0000000000000008h	IMPOSSIBLE	IMPOSSIBLE	IMPOSSIBLE
0000000000000009h	POSSIBLE	POSSIBLE	POSSIBLE
• • •			
FFFFFFFFFFFFFFFEh	POSSIBLE	IMPOSSIBLE	IMPOSSIBLE
FFFFFFFFFFFFFFFFh	IMPOSSIBLE	POSSIBLE	POSSIBLE

FIG.7

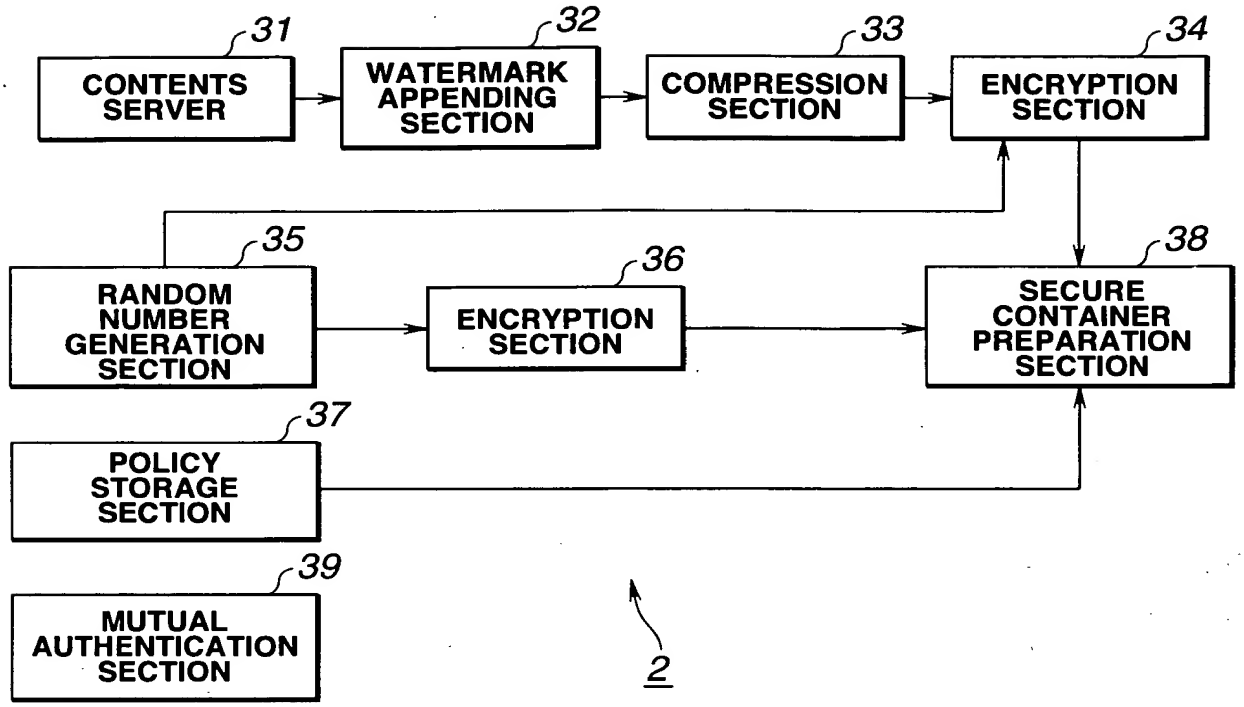
31
CONTENTS SERVER
32
WATERMARK APPENDING SECTION
33
COMPRESSION SECTION
34
ENCRYPTION SECTION
35
RANDOM NUMBER GENERATION SECTION
36
ENCRYPTION SECTION
38
SECURE CONTAINER PREPARATION SECTION
37
POLICY STORAGE SECTION
39
MUTUAL AUTHENTICATION SECTION
2

FIG.8

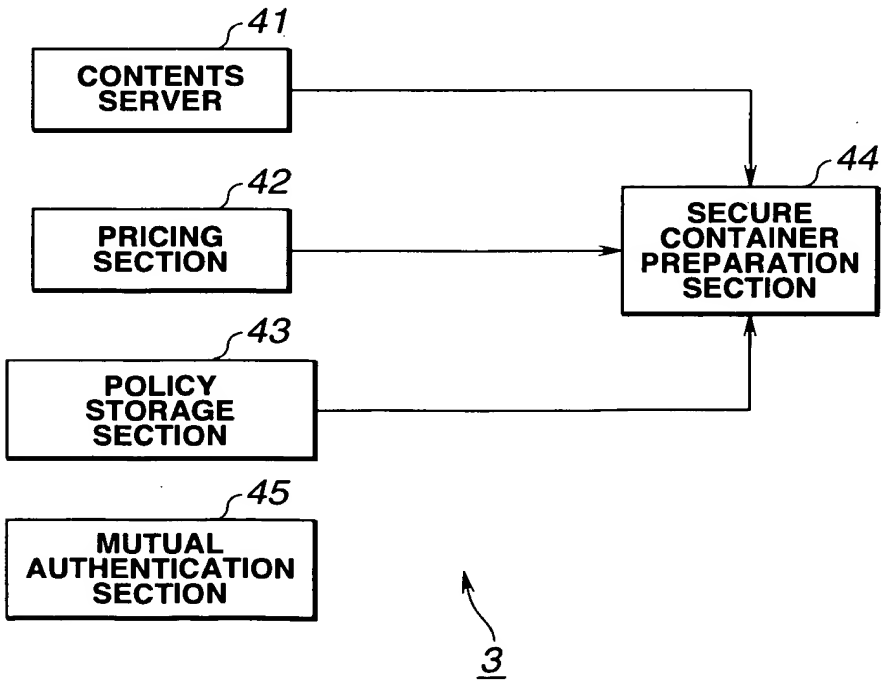
41
CONTENTS SERVER
42
PRICING SECTION
44
SECURE CONTAINER PREPARATION SECTION
43
POLICY STORAGE SECTION
45
MUTUAL AUTHENTICATION SECTION
3

FIG.9

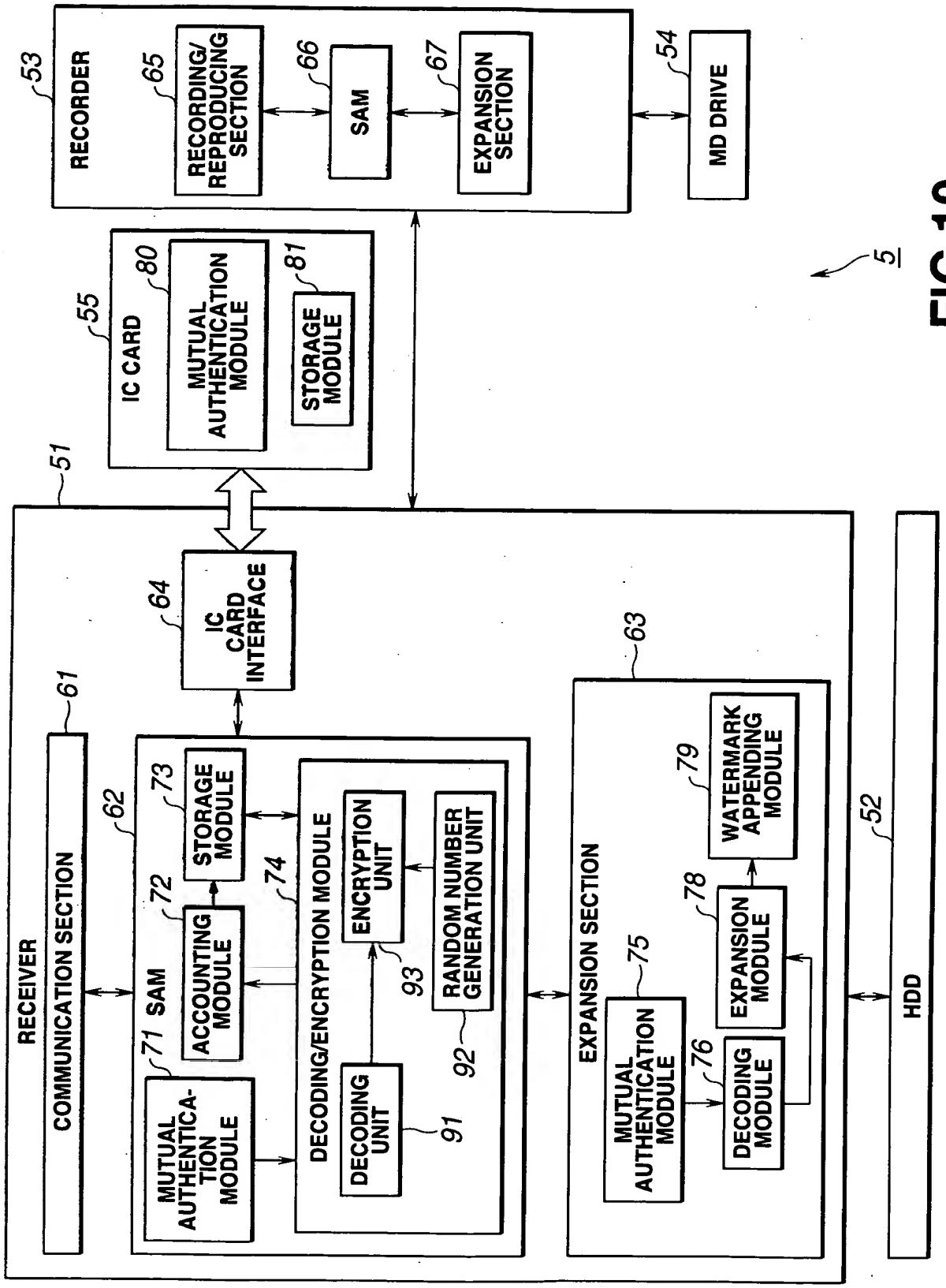
RECORDER
53
RECORDING/ REPRODUCING SECTION
65
SAM
66
EXPANSION SECTION
67
MD DRIVE
54
IC CARD
55
MUTUAL AUTHENTICATION MODULE
80
STORAGE MODULE
81
5
RECEIVER
51
COMMUNICATION SECTION
61
IC CARD INTERFACE
64
SAM
62
MUTUAL AUTHENTICATION MODULE
71
ACCOUNTING MODULE
72
STORAGE MODULE
73
DECODING/ENCRYPTION MODULE
74
DECODING UNIT
91
ENCRYPTION UNIT
93
RANDOM NUMBER GENERATION UNIT
92
EXPANSION SECTION
63
MUTUAL AUTHENTICATION MODULE
75
DECODING MODULE
76
EXPANSION MODULE
78
WATERMARK APPENDING MODULE
79
HDD
52

FIG.10

09/890,583

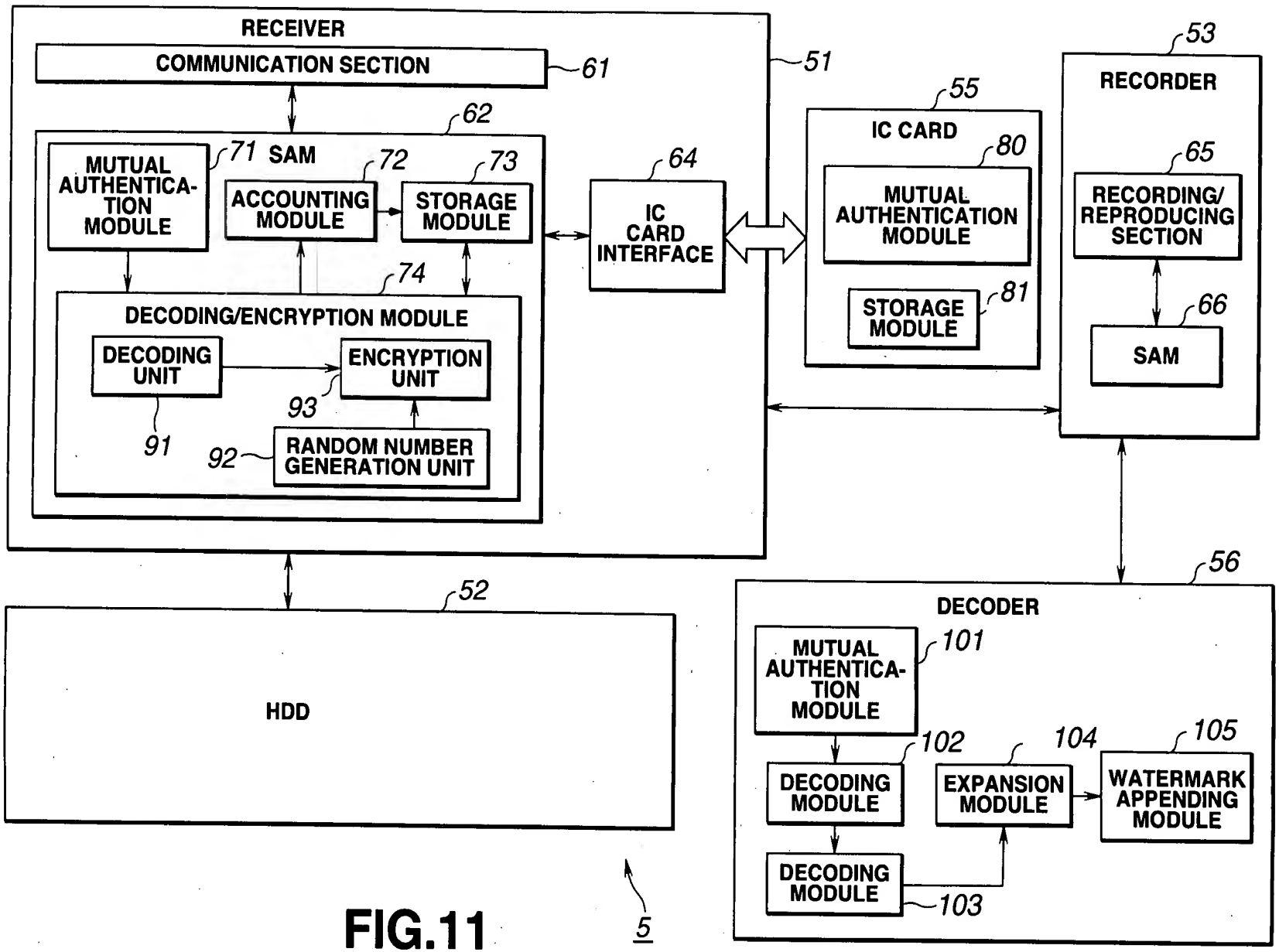

FIG.11

10/88

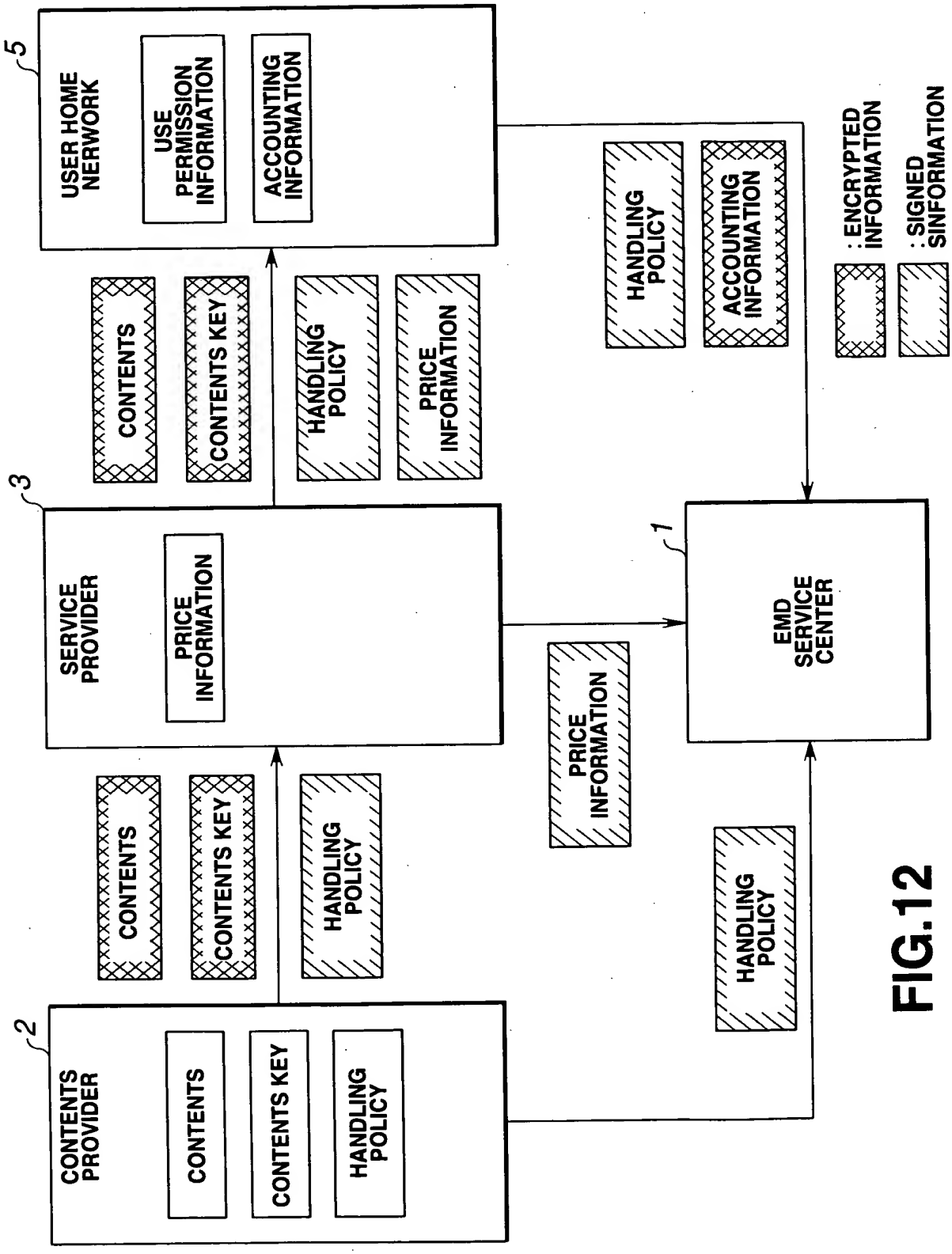
5
USER HOME NERWORK
USE PERMISSION INFORMATION
ACCOUNTING INFORMATION
CONTENTS
CONTENTS KEY
HANDLING POLICY
PRICE INFORMATION
HANDLING POLICY
ACCOUNTING INFORMATION
: ENCRYPTED INFORMATION
: SIGNED SINFORMATION
3
SERVICE PROVIDER
PRICE INFORMATION
1
EMD SERVICE CENTER
PRICE INFORMATION
CONTENTS
CONTENTS KEY
HANDLING POLICY
HANDLING POLICY
2
CONTENTS PROVIDER
CONTENTS
CONTENTS KEY
HANDLING POLICY

FIG.12

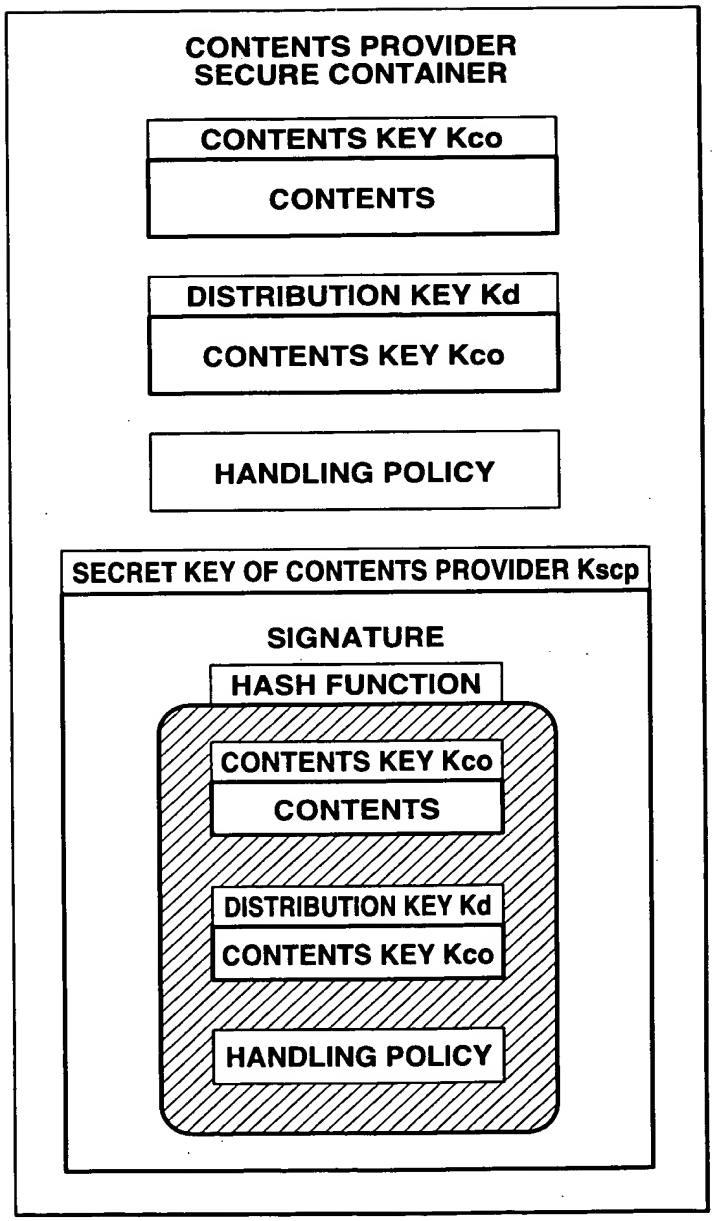
CONTENTS PROVIDER SECURE CONTAINER
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY
SECRET KEY OF CONTENTS PROVIDER Kscp
SIGNATURE
HASH FUNCTION
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY

FIG.13

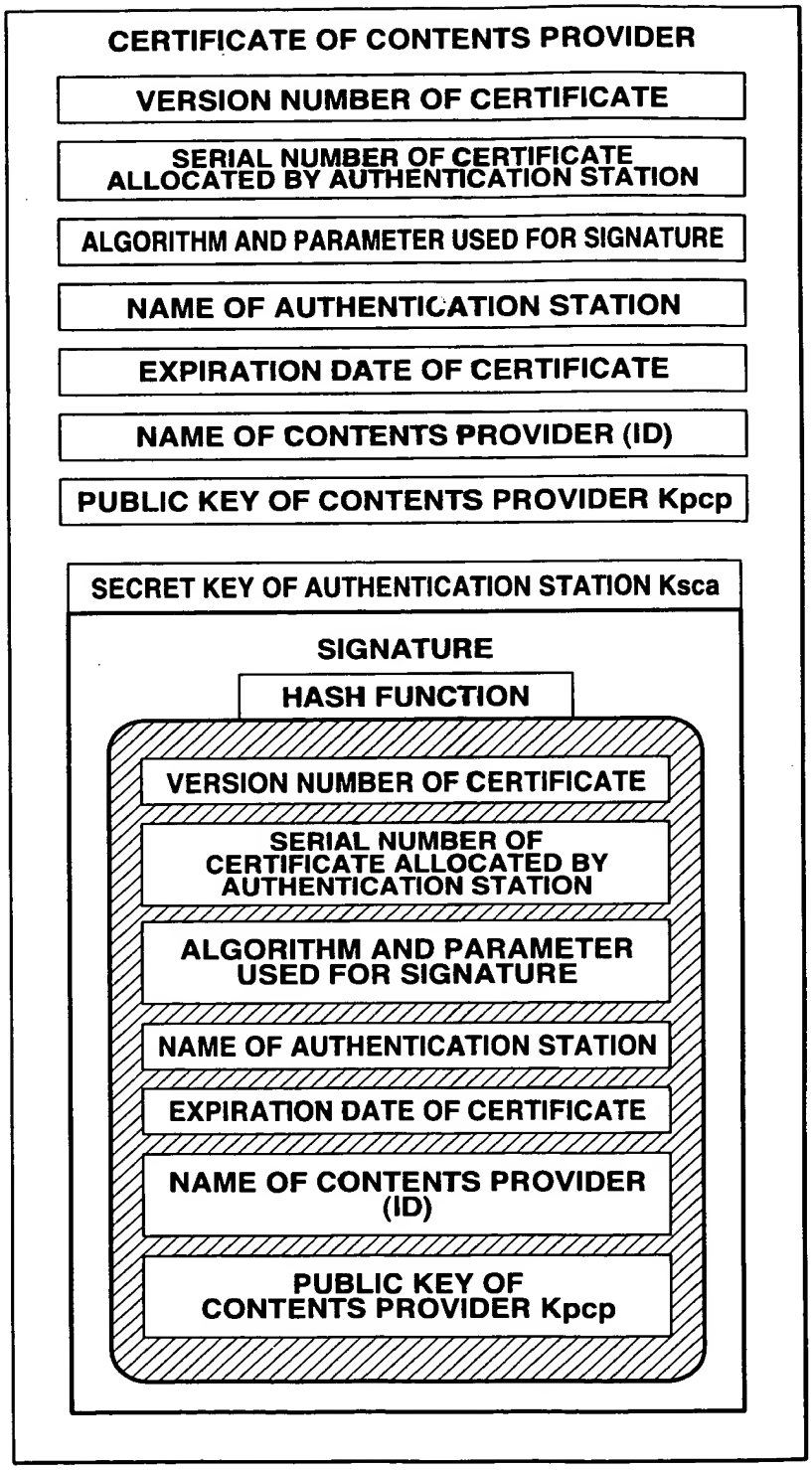
CERTIFICATE OF CONTENTS PROVIDER
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF AUTHENTICATION STATION
EXPIRATION DATE OF CERTIFICATE
NAME OF CONTENTS PROVIDER (ID)
PUBLIC KEY OF CONTENTS PROVIDER Kpcp
SECRET KEY OF AUTHENTICATION STATION Ksca
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF AUTHENTICATION STATION
EXPIRATION DATE OF CERTIFICATE
NAME OF CONTENTS PROVIDER (ID)
PUBLIC KEY OF CONTENTS PROVIDER Kpcp

FIG.14

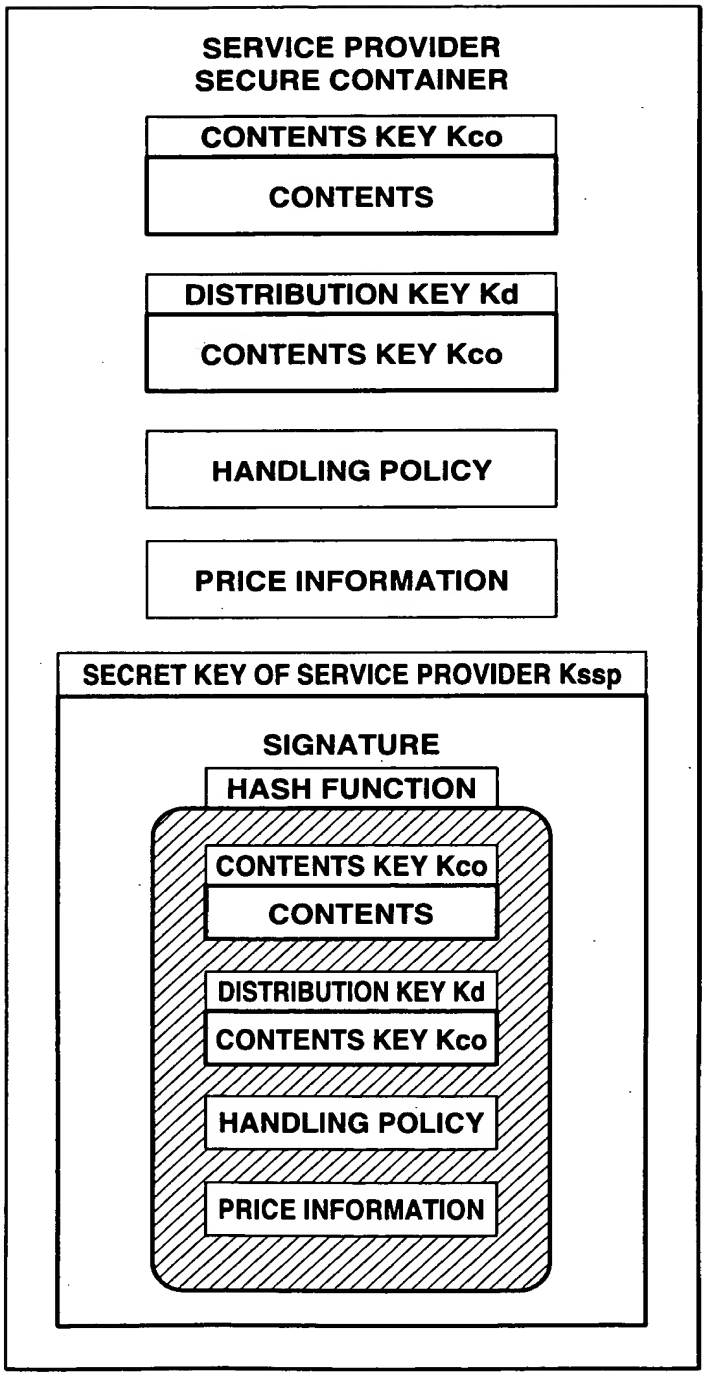
SERVICE PROVIDER
SECURE CONTAINER
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY
PRICE INFORMATION
SECRET KEY OF SERVICE PROVIDER Kssp
SIGNATURE
HASH FUNCTION
CONTENTS KEY Kco
CONTENTS
DISTRIBUTION KEY Kd
CONTENTS KEY Kco
HANDLING POLICY
PRICE INFORMATION

FIG.15

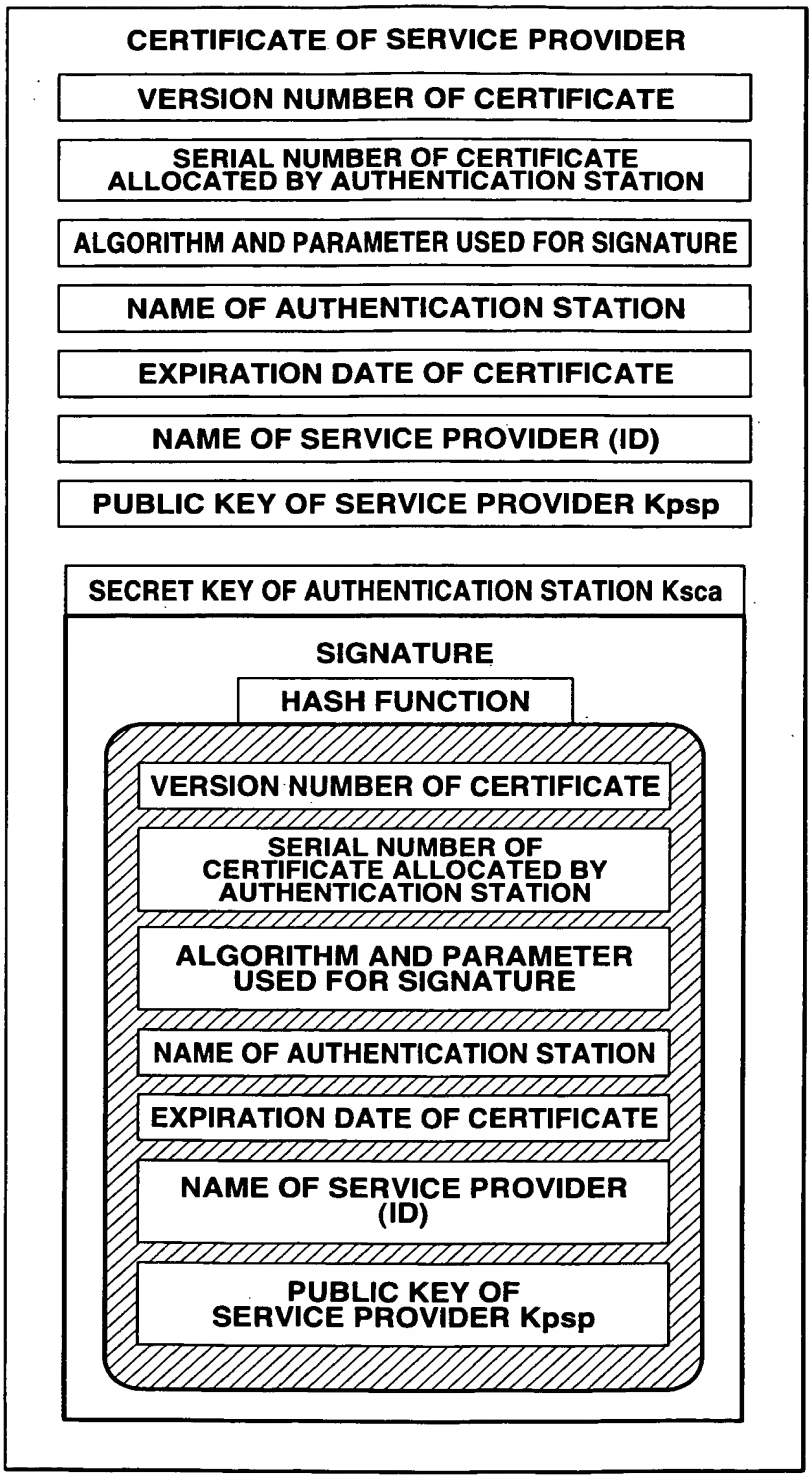

FIG.16

09/581583 - 06/15/00

FIG.17A HANDLING POLICY

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	1	0	1

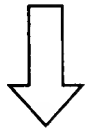

FIG.17B HANDLING POLICY AND PRICE INFORMATION

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	1	0	1
PRICE	150YEN	-	80YEN

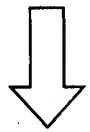

FIG.17C USE PERMISSION INFORMATION

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	1	0	0

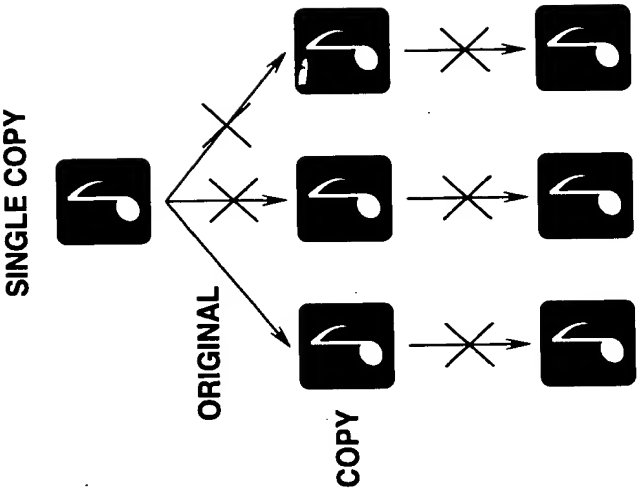

FIG.18B

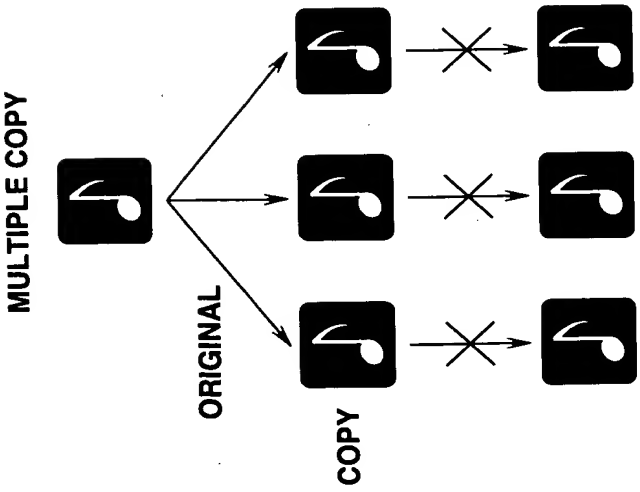

FIG.18A

FIG.19A HANDLING POLICY AND PROFIT DISTRIBUTION

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	1	0	1
PROFIT DISTRIBUTION	70YEN	-	40YEN

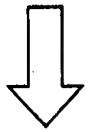

FIG.19B HANDLING POLICY, PROFIT DISTRIBUTION AND PRICE INFORMATION

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
AVAILABILITY	1	0	1
PROFIT DISTRIBUTION	60YEN	-	30YEN
DISTRIBUTION PRICE	150YEN	-	80YEN

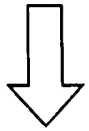

FIG.19C ACCOUNTING INFORMATION

USE	PLAYBACK	SINGLE COPY	MULTIPLE COPY
NUMBER OF TIMES OF USE	1	0	0

09/581583 "PCT/JP98/05960

FIG.20A HANDLING POLICY AND PRICE INFORMATION

USE	PLAY BACK		
	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
	-	5	1998/12/31
PRICE	-	60 YEN	90 YEN

FIG.20B USE PERMISSION INFORMATION

USE	PLAYBACK		
	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
	-	5	-

FIG.20C USE PERMISSION INFORMATION

USE	PLAYBACK		
	UNLIMITED	LIMITED BY NUMBER OF TIMES	LIMITED BY DATE
	-	2	-

09/581583

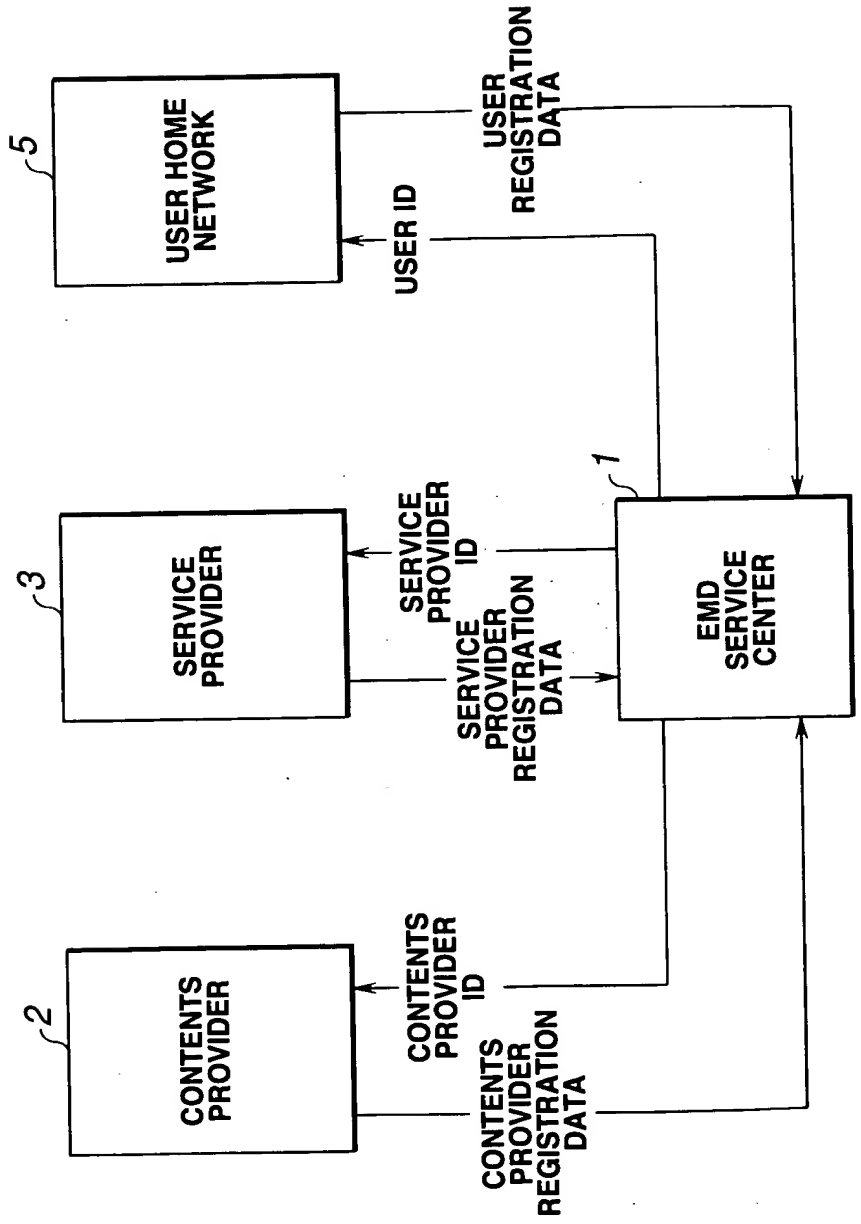
USER HOME NETWORK
5
USER REGISTRATION DATA
USER ID
SERVICE PROVIDER
3
SERVICE PROVIDER ID
SERVICE PROVIDER REGISTRATION DATA
1
EMD SERVICE CENTER
CONTENTS PROVIDER
2
CONTENTS PROVIDER ID
CONTENTS PROVIDER REGISTRATION DATA

FIG.21

CONTENTS ID	CONTENTS PROVIDER ID	ENTITLED ORGANIZATION
1	201	10%
2	201	20%

FIG.22

09581583 060604

00/090"E8ST9S60

PROVIDER ID	CONTENTS ID	DISCOUNT RATE	PERIOD
CONTENTS PROVIDER 1	1	2%	1998.9~1998.12
	2	3%	
	ALL CONTENTS	1%	
CONTENTS PROVIDER 2	3	5%	
SERVICE PROVIDER 1	1	3%	
SERVICE PROVIDER 2	4	1%	

FIG.23

09/581583

MONTHLY FIXED RATE	VARIABLE RATE		
1000YEN	PERIOD	1998.8～1998.9	-10%
	FEE	3000YEN OR MORE	-5%

FIG.24

09581583 082599

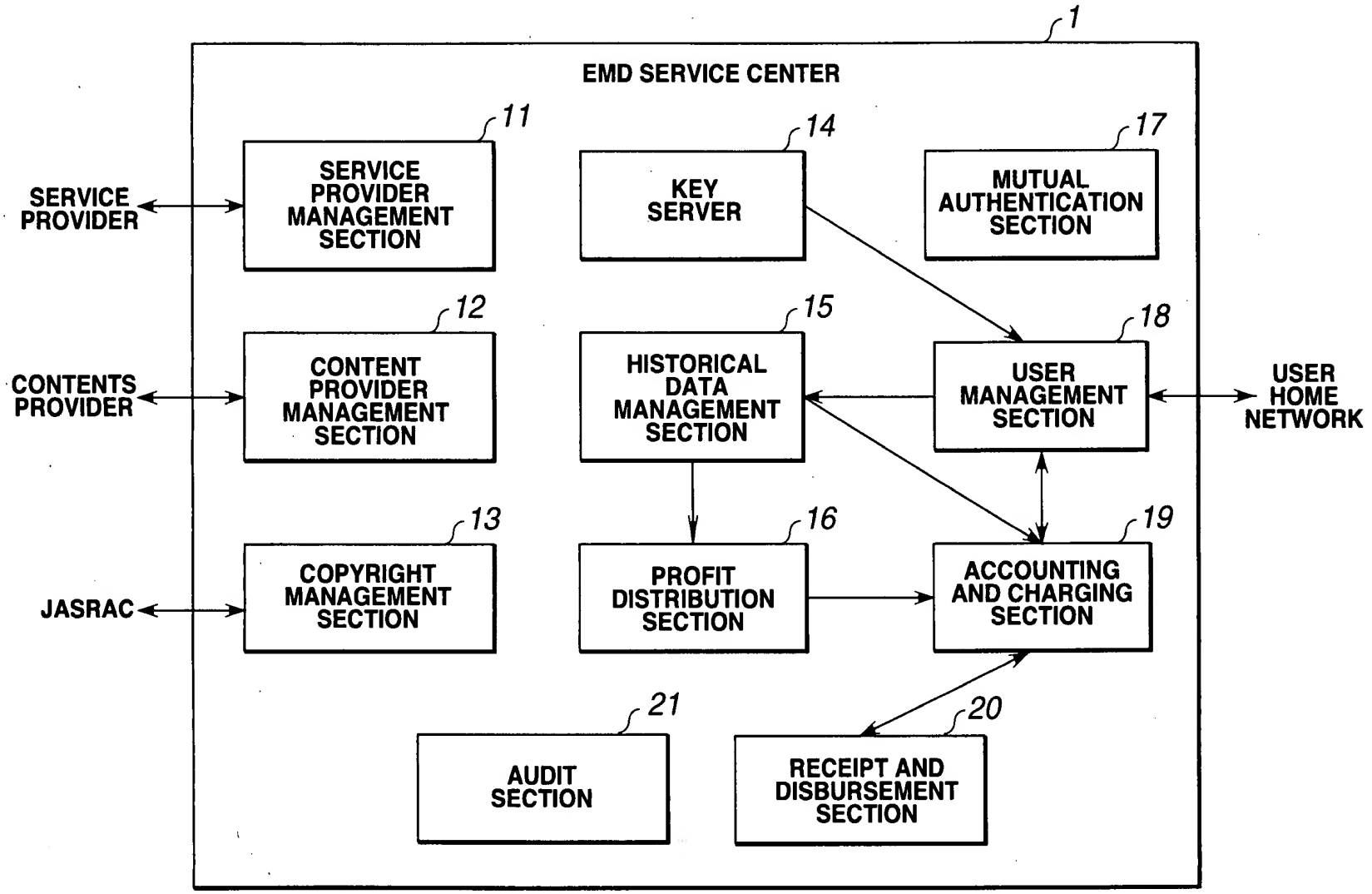

FIG.25

09/581583

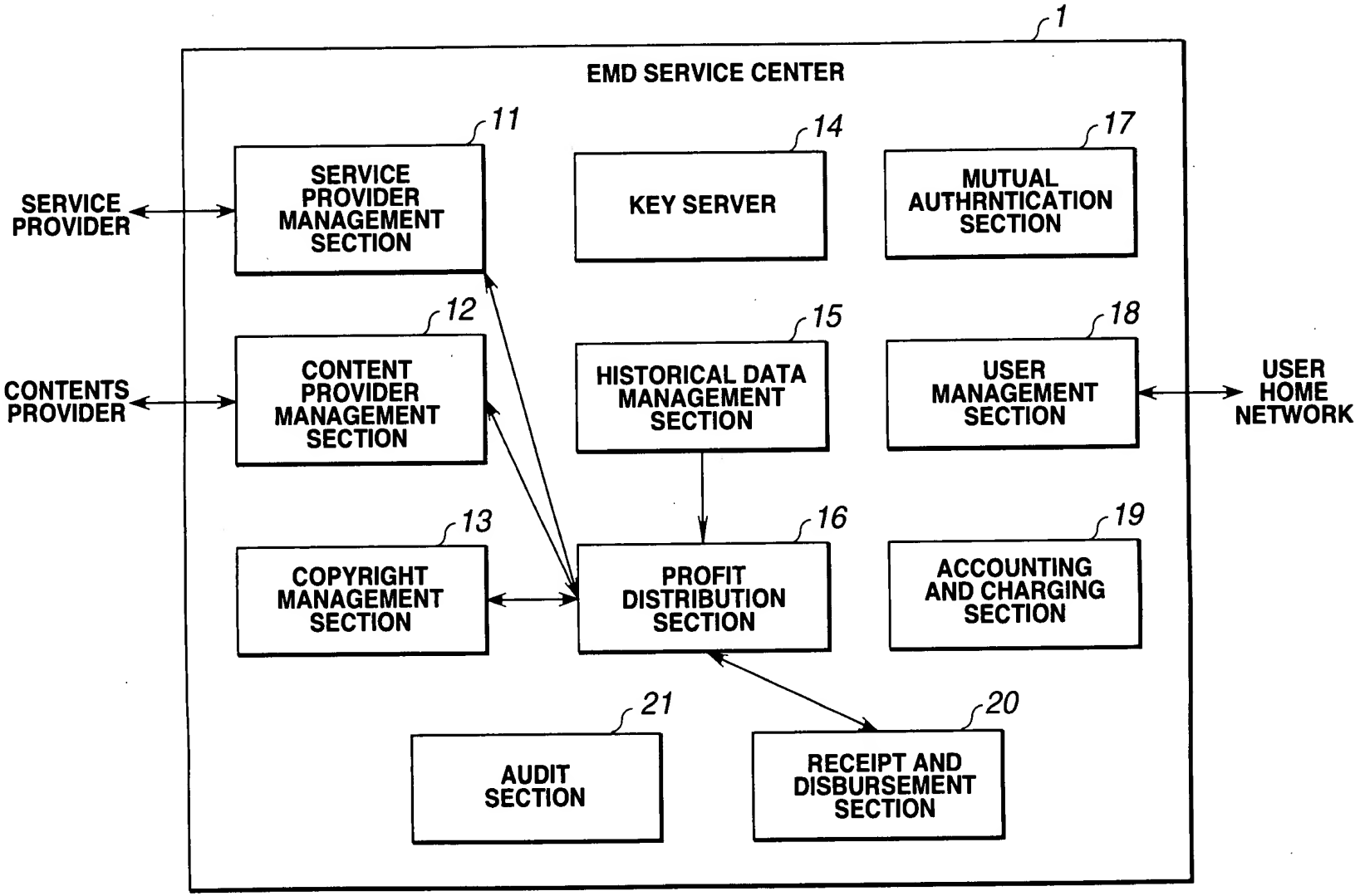

FIG.26

09/581583

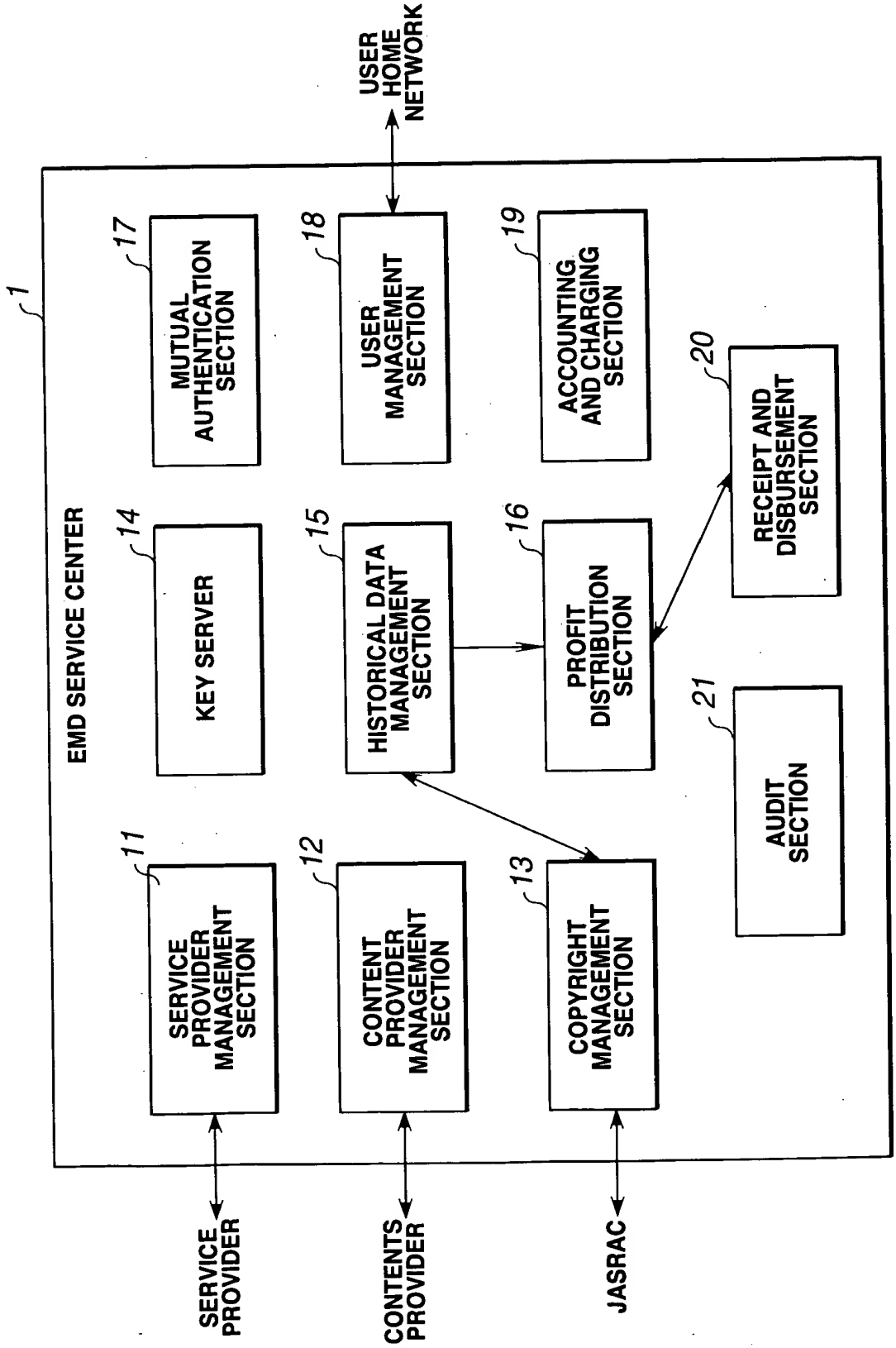
USER HOME NETWORK
1
EMD SERVICE CENTER
17
MUTUAL AUTHENTICATION SECTION
18
USER MANAGEMENT SECTION
19
ACCOUNTING AND CHARGING SECTION
20
RECEIPT AND DISBURSEMENT SECTION
14
KEY SERVER
15
HISTORICAL DATA MANAGEMENT SECTION
16
PROFIT DISTRIBUTION SECTION
21
AUDIT SECTION
11
SERVICE PROVIDER MANAGEMENT SECTION
12
CONTENT PROVIDER MANAGEMENT SECTION
13
COPYRIGHT MANAGEMENT SECTION
SERVICE PROVIDER
CONTENTS PROVIDER
JASRAC

FIG.27

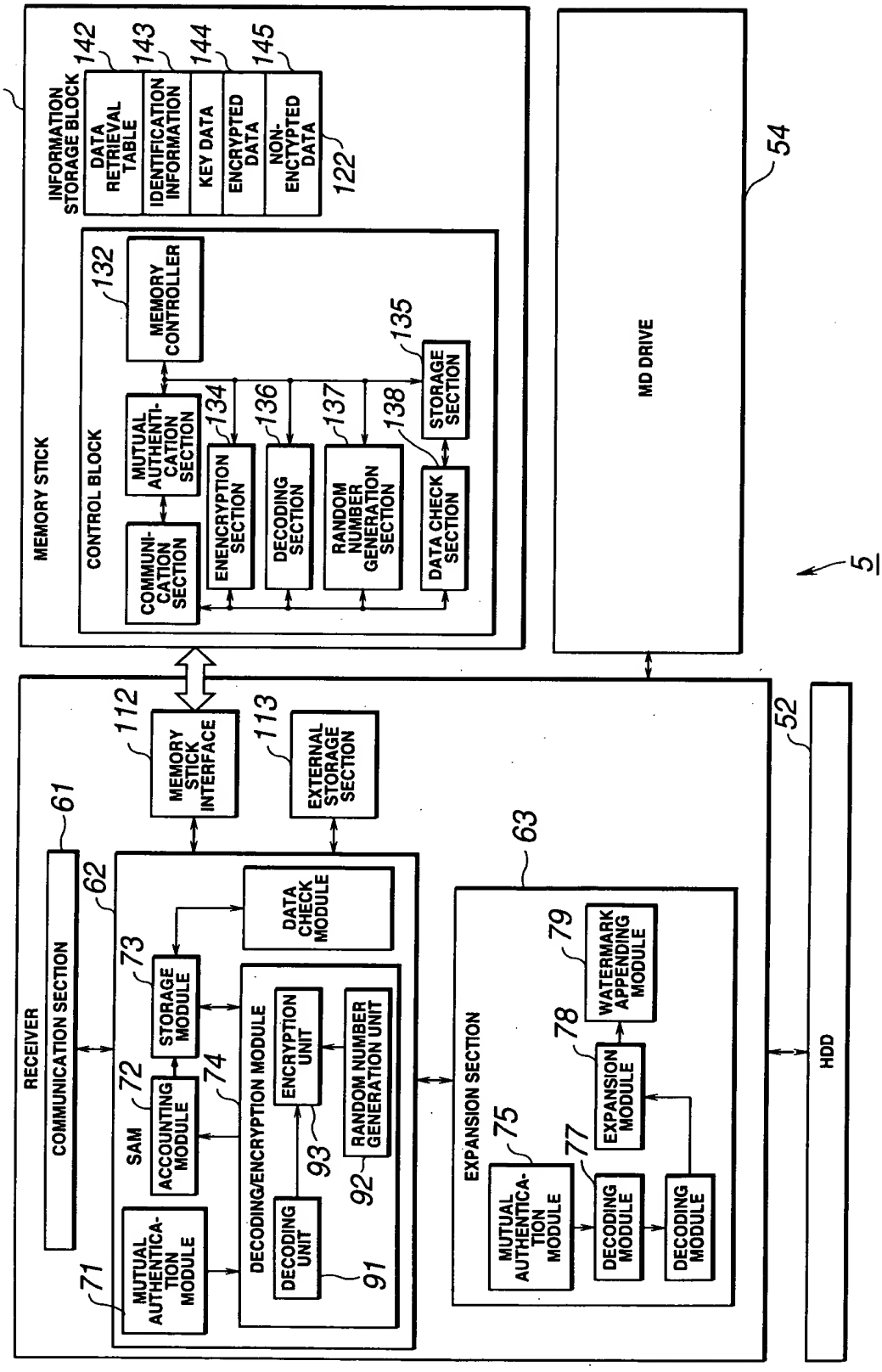
111
MEMORY STICK
INFORMATION STORAGE BLOCK
142
DATA RETRIEVAL TABLE
143
IDENTIFICATION INFORMATION
144
KEY DATA
145
ENCRYPTED DATA
NON-ENCTYPTED DATA
122
CONTROL BLOCK
132
MEMORY CONTROLLER
MUTUAL AUTHENTI-CATION SECTION
134
136
137
138
135
STORAGE SECTION
COMMUNI-CATION SECTION
ENENCRYPTION SECTION
DECODING SECTION
RANDOM NUMBER GENERATION SECTION
DATA CHECK SECTION
MD DRIVE
54
5
112
MEMORY STICK INTERFACE
113
EXTERNAL STORAGE SECTION
61
RECEIVER
COMMUNICATION SECTION
62
SAM
72
ACCOUNTING MODULE
73
STORAGE MODULE
74
DATA CHECK MODULE
DECODING/ENCRYPTION MODULE
ENCRYPTION UNIT
RANDOM NUMBER GENERATION UNIT
93
92
DECODING UNIT
91
71
MUTUAL AUTHENTICA-TION MODULE
63
EXPANSION SECTION
75
MUTUAL AUTHENTICA-TION MODULE
77
DECODING MODULE
DECODING MODULE
78
EXPANSION MODULE
79
WATERMARK APPENDING MODULE
52
HDD

FIG.28

09/581583

KEY DATA BLOCK 1	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
KEY DATA BLOCK 2	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
KEY DATA BLOCK 3	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4				CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6
KEY DATA BLOCK 5						

FIG.29

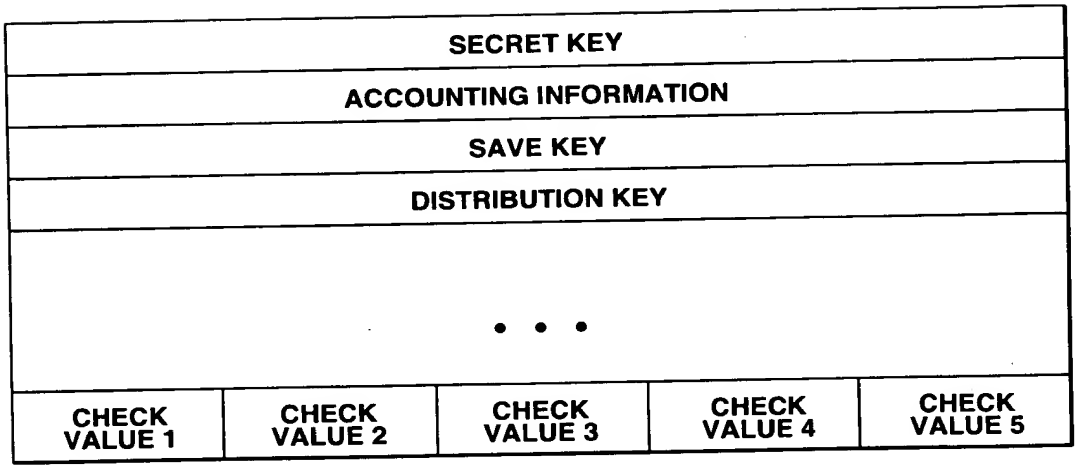
SECRET KEY
ACCOUNTING INFORMATION
SAVE KEY
DISTRIBUTION KEY
• • •
CHECK VALUE 1
CHECK VALUE 2
CHECK VALUE 3
CHECK VALUE 4
CHECK VALUE 5

FIG.30

KEY DATA BLOCK 1	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
KEY DATA BLOCK 2	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
KEY DATA BLOCK 3	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4				CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6
KEY DATA BLOCK 5						
	CHECK VALUE 1	CHECK VALUE 2	CHECK VALUE 3	CHECK VALUE 4	CHECK VALUE 5	

FIG.31

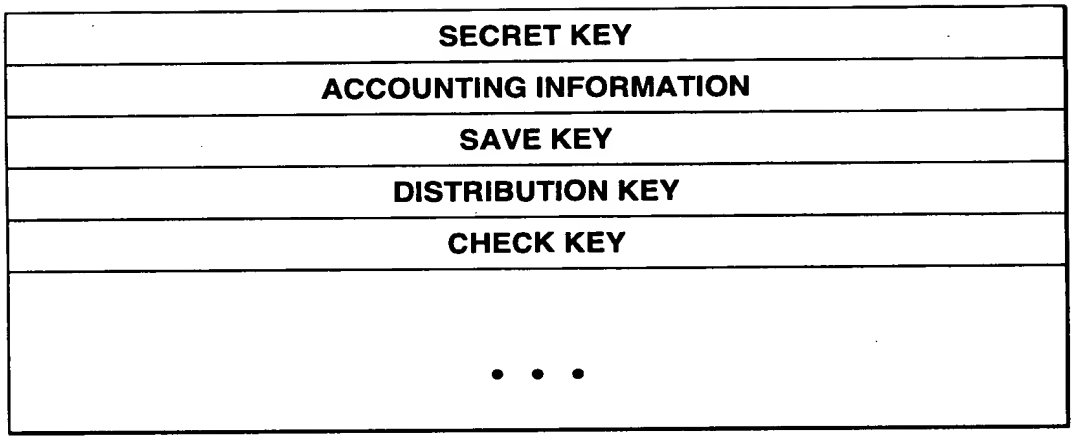
SECRET KEY
ACCOUNTING INFORMATION
SAVE KEY
DISTRIBUTION KEY
CHECK KEY
• • •

FIG.32

09/581583 032788

KEY DATA BLOCK 1	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
KEY DATA BLOCK 2	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
KEY DATA BLOCK 3	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4	CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6			

FIG.33

09/581583 032788

09581583 062600

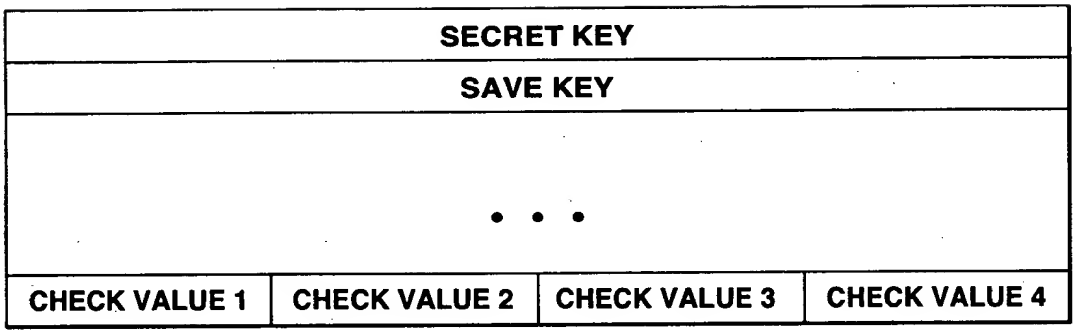

FIG.34

09/581583 "EB511659"

KEY DATA BLOCK 1	CONTENTS KEY 1	CONTENTS ID 1	USE PERMISSION INFORMATION 1	CONTENTS KEY 2	CONTENTS ID 2	USE PERMISSION INFORMATION 2
KEY DATA BLOCK 2	CONTENTS KEY 3	CONTENTS ID 3	USE PERMISSION INFORMATION 3	CONTENTS KEY 4	CONTENTS ID 4	USE PERMISSION INFORMATION 4
KEY DATA BLOCK 3	CONTENTS KEY 5	CONTENTS ID 5	USE PERMISSION INFORMATION 5			
KEY DATA BLOCK 4	CONTENTS KEY 6	CONTENTS ID 6	USE PERMISSION INFORMATION 6			
	CHECK VALUE 1		CHECK VALUE 2	CHECK VALUE 3		CHECK VALUE 4

FIG.35

09/581583

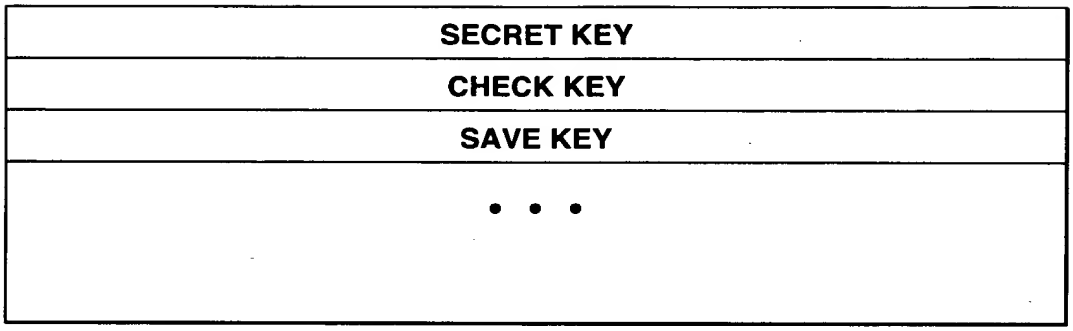

FIG.36

09/581583 060500

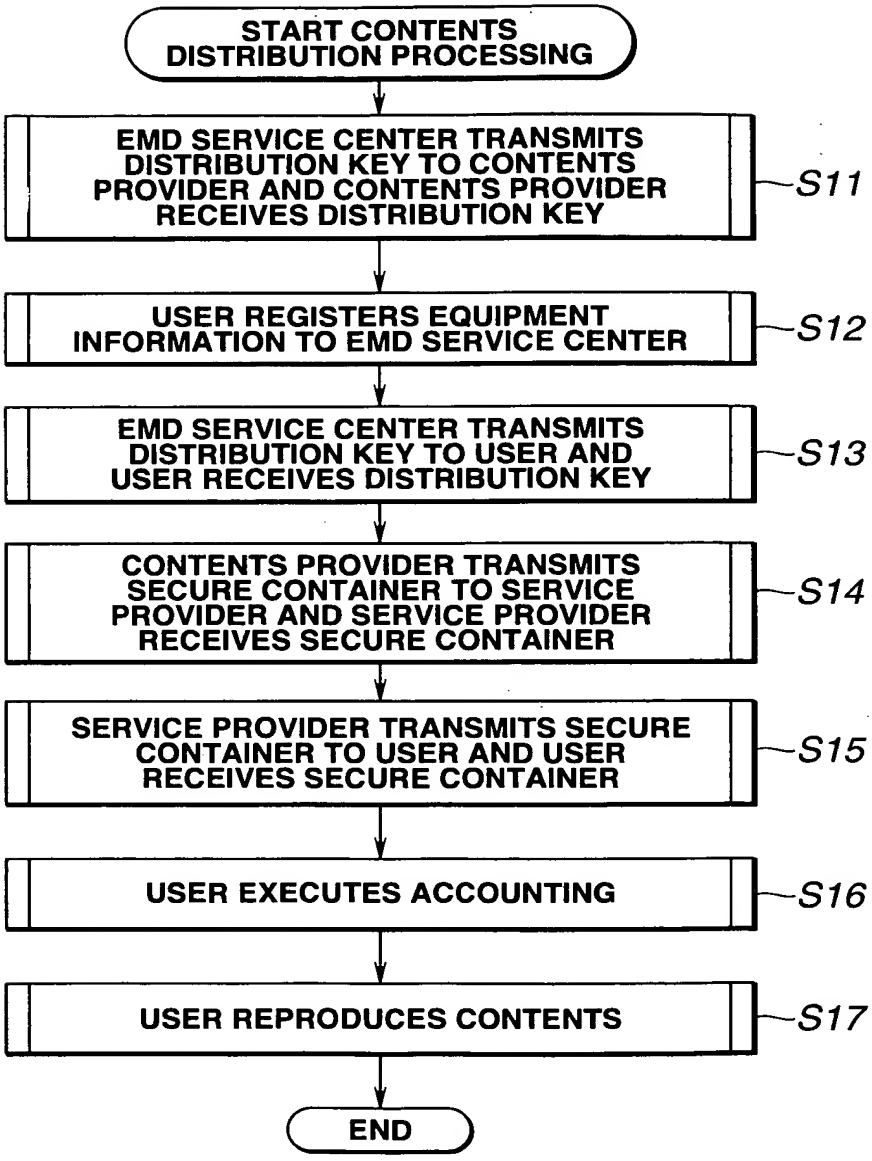
START CONTENTS DISTRIBUTION PROCESSING
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY TO CONTENTS PROVIDER AND CONTENTS PROVIDER RECEIVES DISTRIBUTION KEY
S11
USER REGISTERS EQUIPMENT INFORMATION TO EMD SERVICE CENTER
S12
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY TO USER AND USER RECEIVES DISTRIBUTION KEY
S13
CONTENTS PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE PROVIDER AND SERVICE PROVIDER RECEIVES SECURE CONTAINER
S14
SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER AND USER RECEIVES SECURE CONTAINER
S15
USER EXECUTES ACCOUNTING
S16
USER REPRODUCES CONTENTS
S17
END

FIG.37

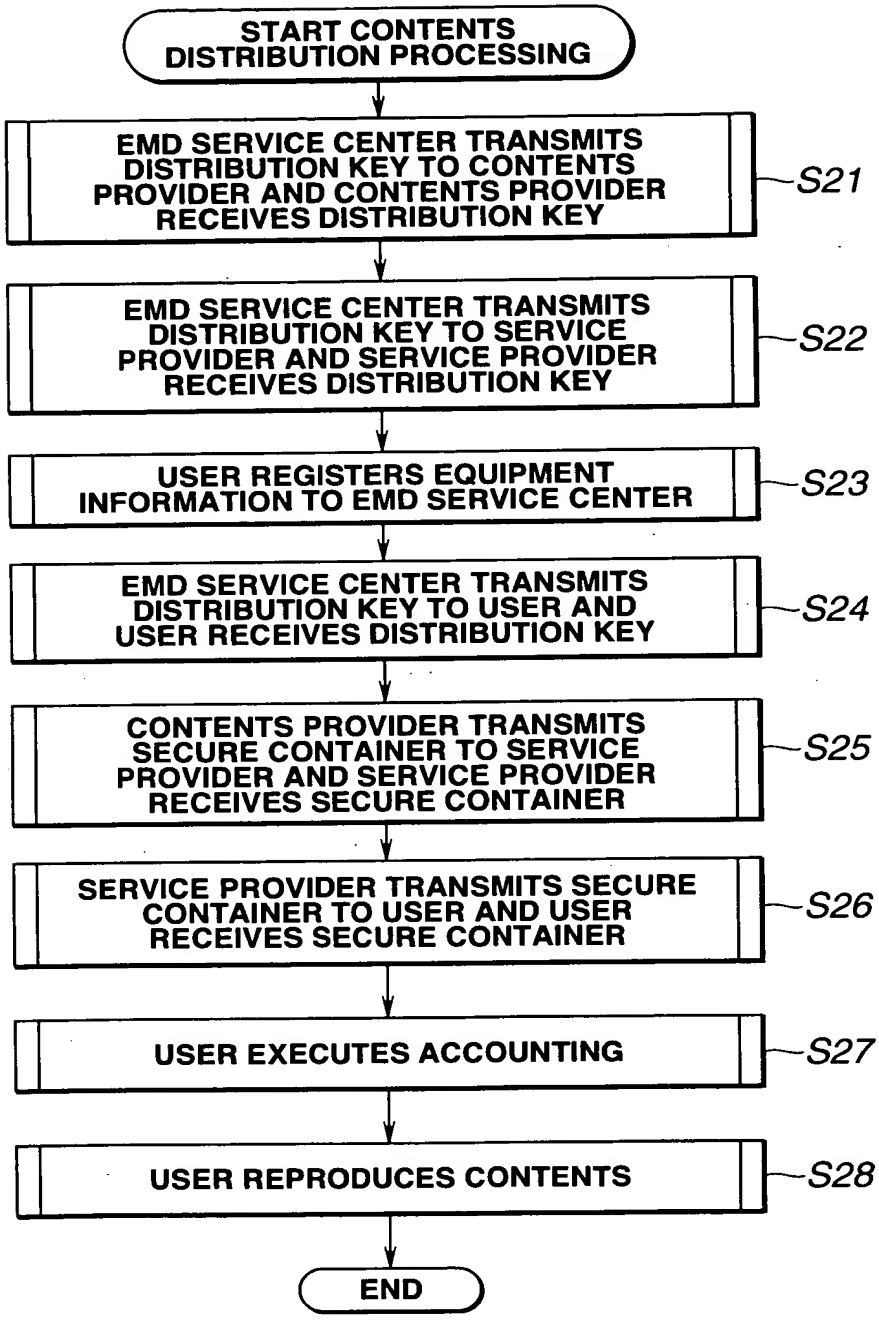
START CONTENTS DISTRIBUTION PROCESSING
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY TO CONTENTS PROVIDER AND CONTENTS PROVIDER RECEIVES DISTRIBUTION KEY
S21
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY TO SERVICE PROVIDER AND SERVICE PROVIDER RECEIVES DISTRIBUTION KEY
S22
USER REGISTERS EQUIPMENT INFORMATION TO EMD SERVICE CENTER
S23
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY TO USER AND USER RECEIVES DISTRIBUTION KEY
S24
CONTENTS PROVIDER TRANSMITS SECURE CONTAINER TO SERVICE PROVIDER AND SERVICE PROVIDER RECEIVES SECURE CONTAINER
S25
SERVICE PROVIDER TRANSMITS SECURE CONTAINER TO USER AND USER RECEIVES SECURE CONTAINER
S26
USER EXECUTES ACCOUNTING
S27
USER REPRODUCES CONTENTS
S28
END

FIG.38

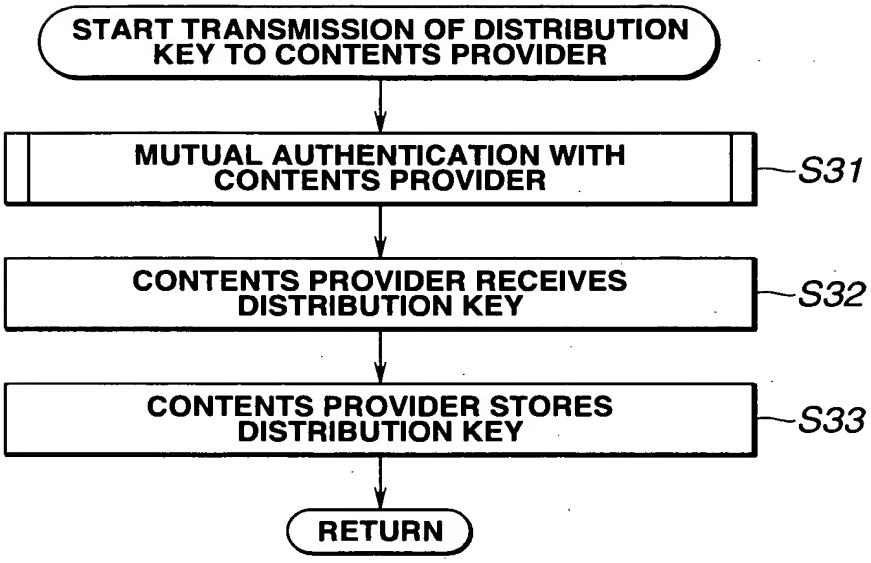
START TRANSMISSION OF DISTRIBUTION KEY TO CONTENTS PROVIDER
MUTUAL AUTHENTICATION WITH CONTENTS PROVIDER
S31
CONTENTS PROVIDER RECEIVES DISTRIBUTION KEY
S32
CONTENTS PROVIDER STORES DISTRIBUTION KEY
S33
RETURN

FIG.39

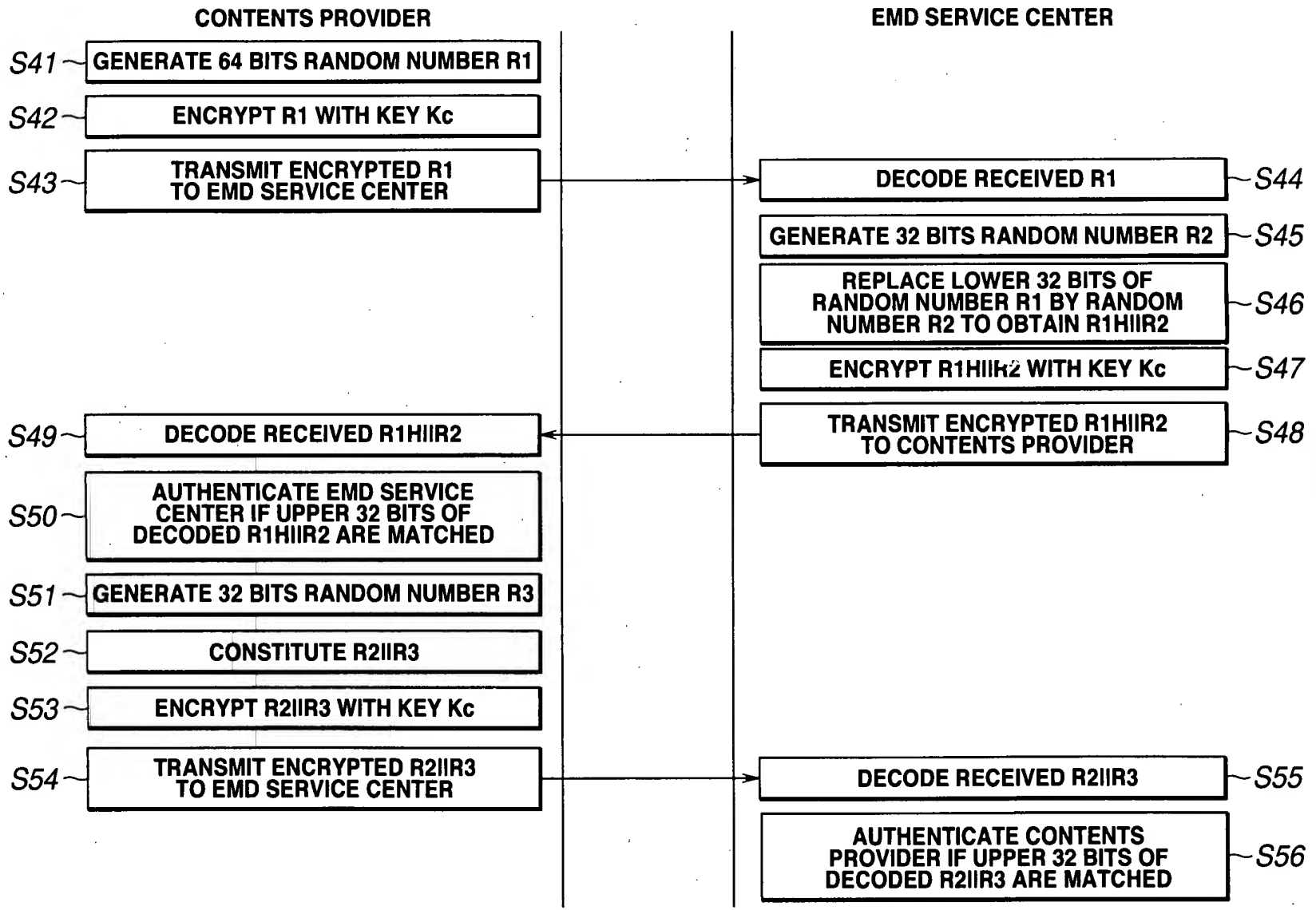
CONTENTS PROVIDER
EMD SERVICE CENTER
S41
GENERATE 64 BITS RANDOM NUMBER R1
S42
ENCRYPT R1 WITH KEY Kc
S43
TRANSMIT ENCRYPTED R1 TO EMD SERVICE CENTER
DECODE RECEIVED R1
S44
GENERATE 32 BITS RANDOM NUMBER R2
S45
REPLACE LOWER 32 BITS OF RANDOM NUMBER R1 BY RANDOM NUMBER R2 TO OBTAIN R1HIIR2
S46
ENCRYPT R1HIIR2 WITH KEY Kc
S47
TRANSMIT ENCRYPTED R1HIIR2 TO CONTENTS PROVIDER
S48
S49
DECODE RECEIVED R1HIIR2
S50
AUTHENTICATE EMD SERVICE CENTER IF UPPER 32 BITS OF DECODED R1HIIR2 ARE MATCHED
S51
GENERATE 32 BITS RANDOM NUMBER R3
S52
CONSTITUTE R2IIR3
S53
ENCRYPT R2IIR3 WITH KEY Kc
S54
TRANSMIT ENCRYPTED R2IIR3 TO EMD SERVICE CENTER
DECODE RECEIVED R2IIR3
S55
AUTHENTICATE CONTENTS PROVIDER IF UPPER 32 BITS OF DECODED R2IIR3 ARE MATCHED
S56

FIG.40

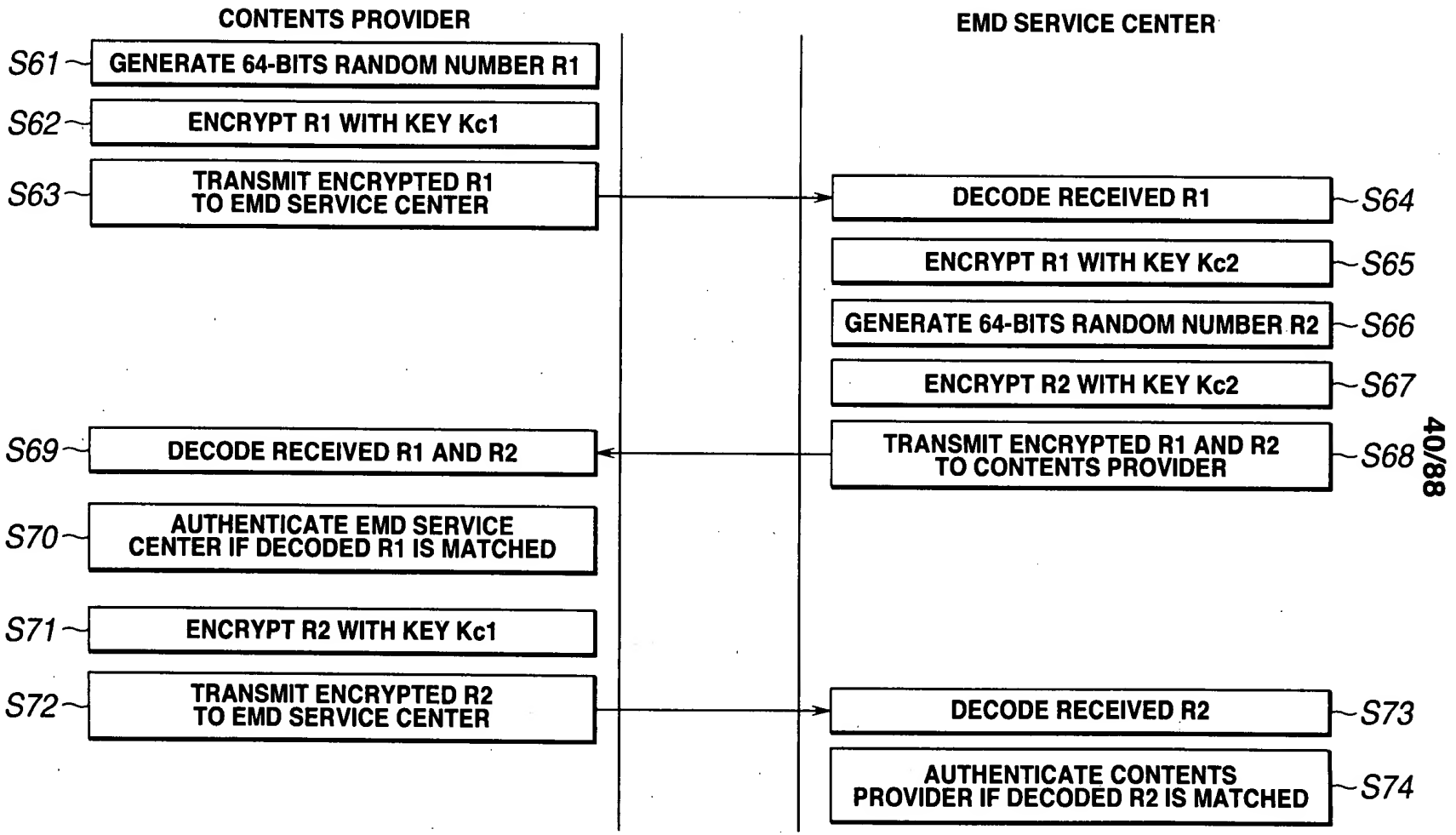

FIG.41

09/581583

09/581583

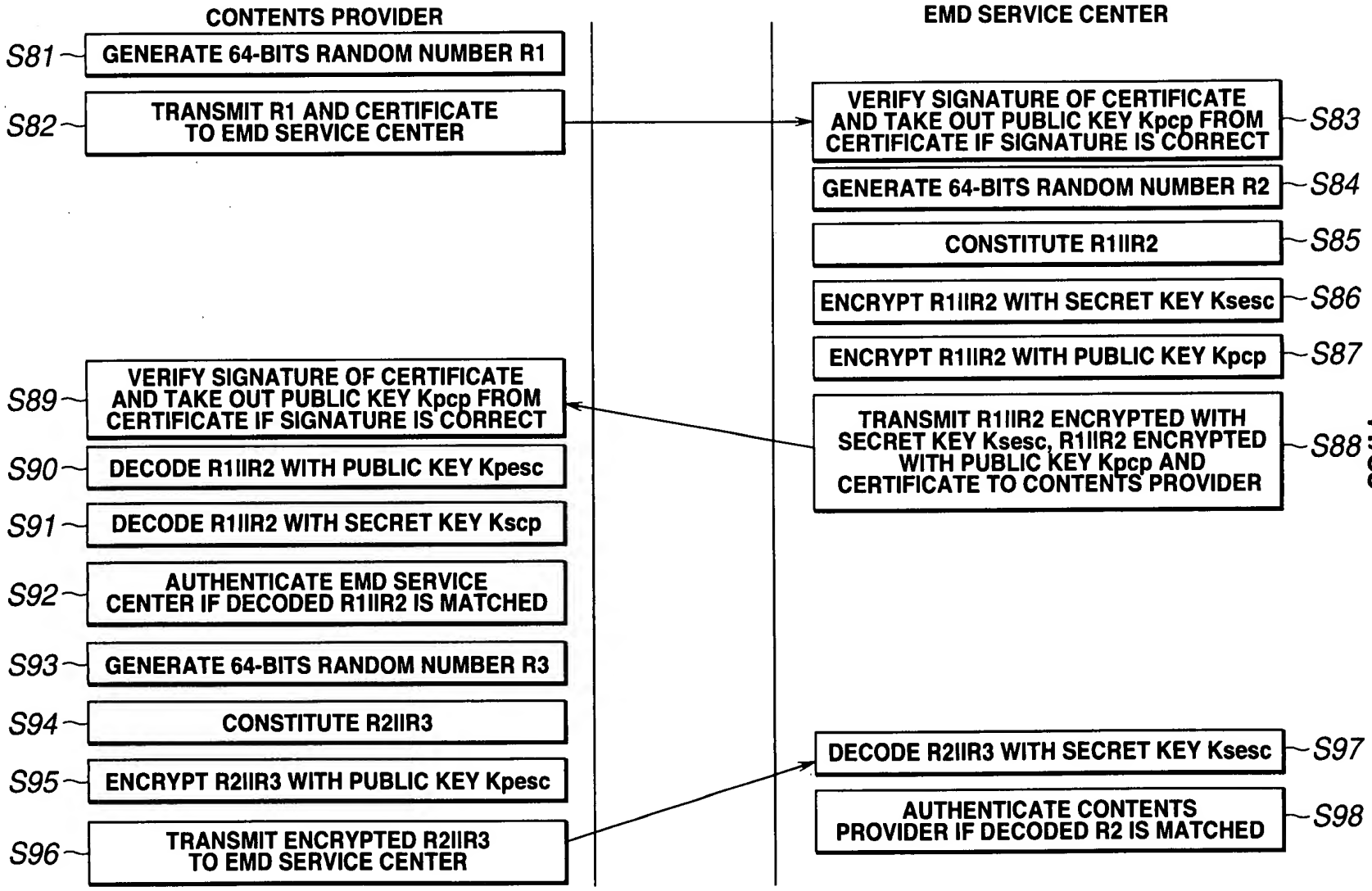

FIG.42

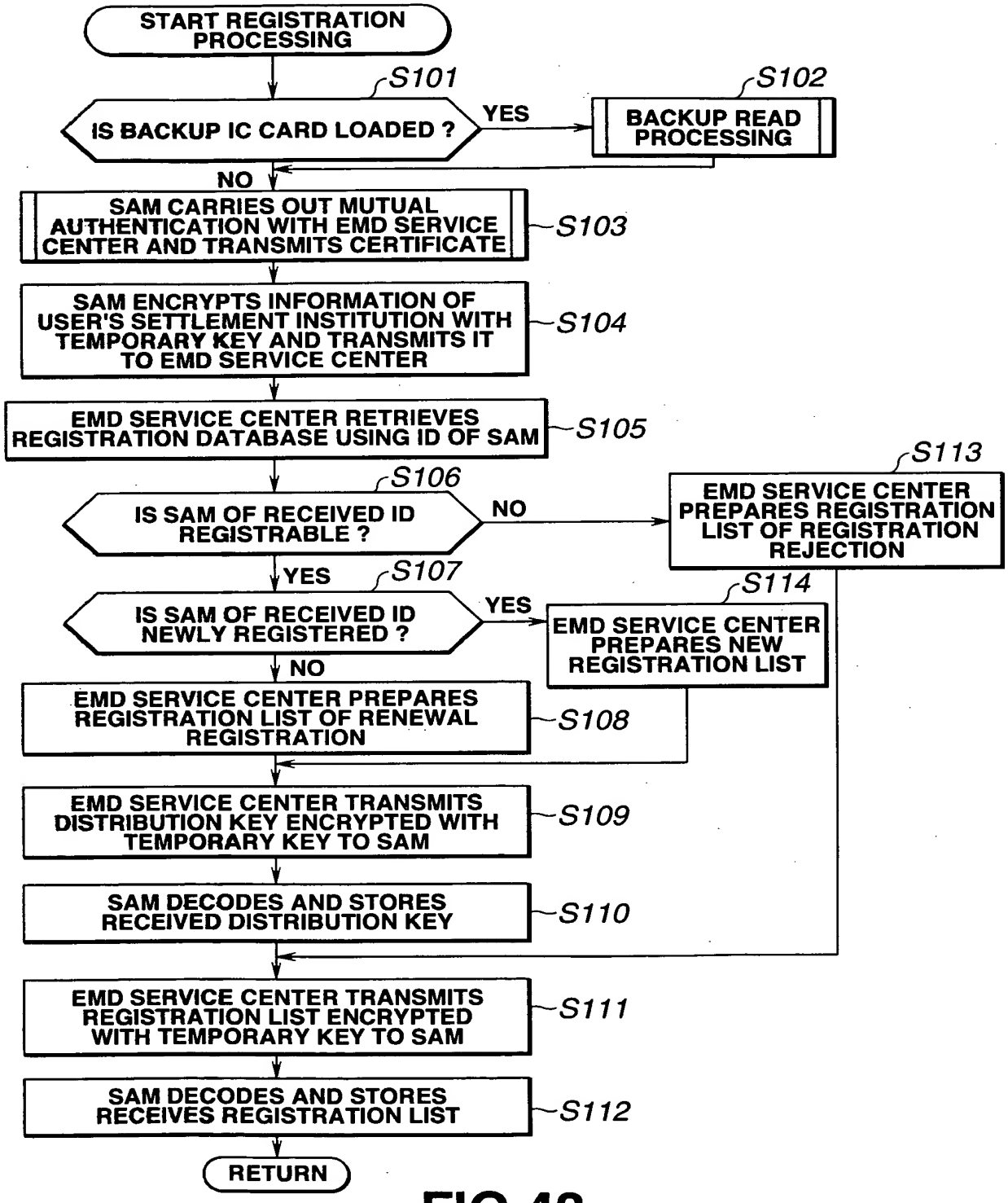
START REGISTRATION PROCESSING
S101
IS BACKUP IC CARD LOADED ?
YES
S102
BACKUP READ PROCESSING
NO
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER AND TRANSMITS CERTIFICATE
S103
SAM ENCRYPTS INFORMATION OF USER'S SETTLEMENT INSTITUTION WITH TEMPORARY KEY AND TRANSMITS IT TO EMD SERVICE CENTER
S104
EMD SERVICE CENTER RETRIEVES REGISTRATION DATABASE USING ID OF SAM
S105
S106
IS SAM OF RECEIVED ID REGISTRABLE ?
NO
S113
EMD SERVICE CENTER PREPARES REGISTRATION LIST OF REGISTRATION REJECTION
YES
S107
IS SAM OF RECEIVED ID NEWLY REGISTERED ?
YES
S114
EMD SERVICE CENTER PREPARES NEW REGISTRATION LIST
NO
EMD SERVICE CENTER PREPARES REGISTRATION LIST OF RENEWAL REGISTRATION
S108
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY ENCRYPTED WITH TEMPORARY KEY TO SAM
S109
SAM DECODES AND STORES RECEIVED DISTRIBUTION KEY
S110
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY TO SAM
S111
SAM DECODES AND STORES RECEIVES REGISTRATION LIST
S112
RETURN

FIG.43

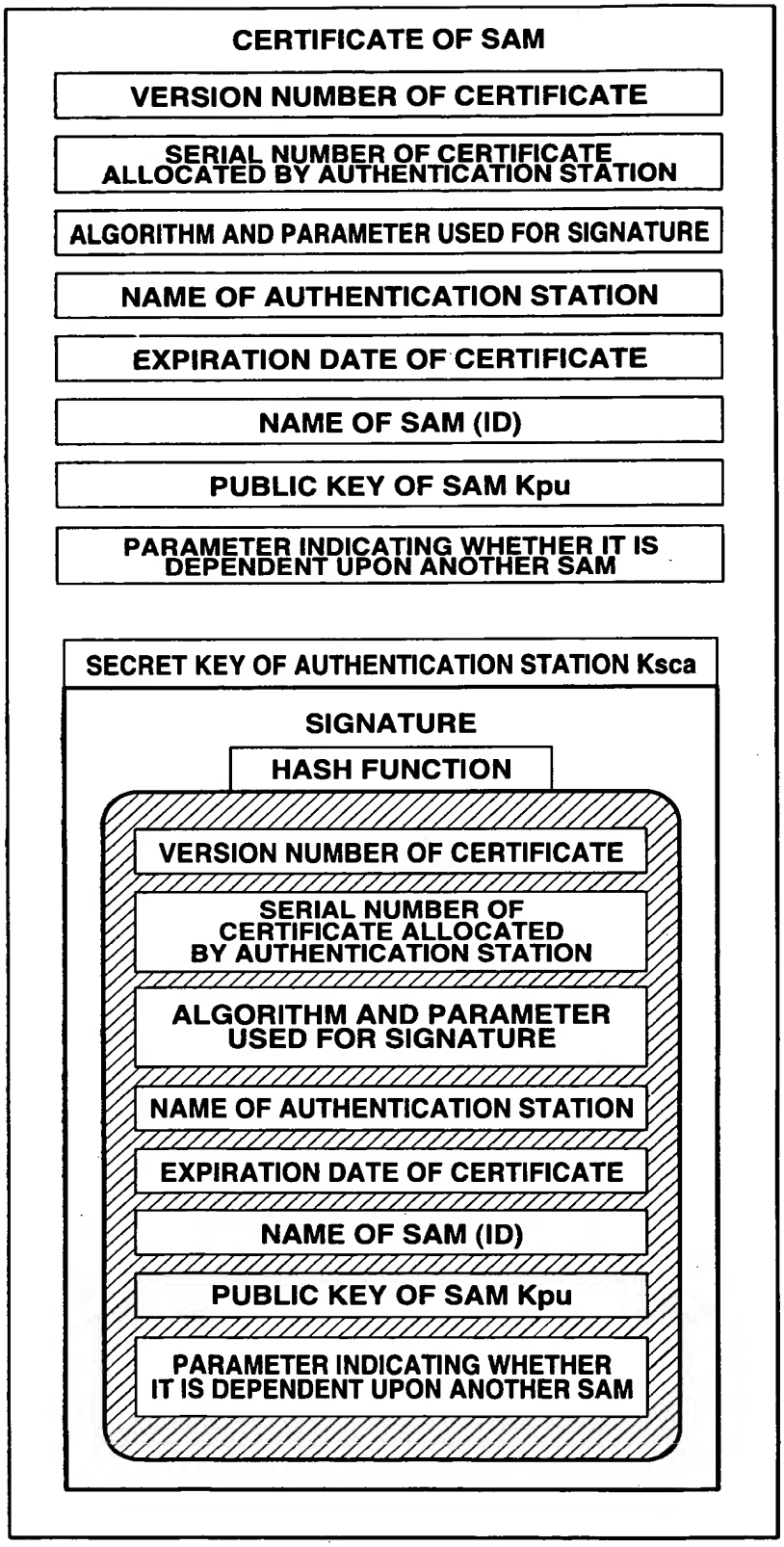
CERTIFICATE OF SAM
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF AUTHENTICATION STATION
EXPIRATION DATE OF CERTIFICATE
NAME OF SAM (ID)
PUBLIC KEY OF SAM Kpu
PARAMETER INDICATING WHETHER IT IS DEPENDENT UPON ANOTHER SAM
SECRET KEY OF AUTHENTICATION STATION Ksca
SIGNATURE
HASH FUNCTION
VERSION NUMBER OF CERTIFICATE
SERIAL NUMBER OF CERTIFICATE ALLOCATED BY AUTHENTICATION STATION
ALGORITHM AND PARAMETER USED FOR SIGNATURE
NAME OF AUTHENTICATION STATION
EXPIRATION DATE OF CERTIFICATE
NAME OF SAM (ID)
PUBLIC KEY OF SAM Kpu
PARAMETER INDICATING WHETHER IT IS DEPENDENT UPON ANOTHER SAM

FIG.44

ID OF SAM (64 BITS)	REGISTRATION REJECTION FLAG (1 BIT)	STATUS FLAG (4 BITS)	CONDITION FLAG (1 BIT)	SIGNATURE
0000000000000001h	1	0000	0	xxxxxxxxxx
0000000000000002h	1	1010	1	xxxxxxxxxx
0000000000000003h	1	1100	1	xxxxxxxxxx
000000000000000Ah	0	0000	1	xxxxxxxxxx

FIG.45

09/581583

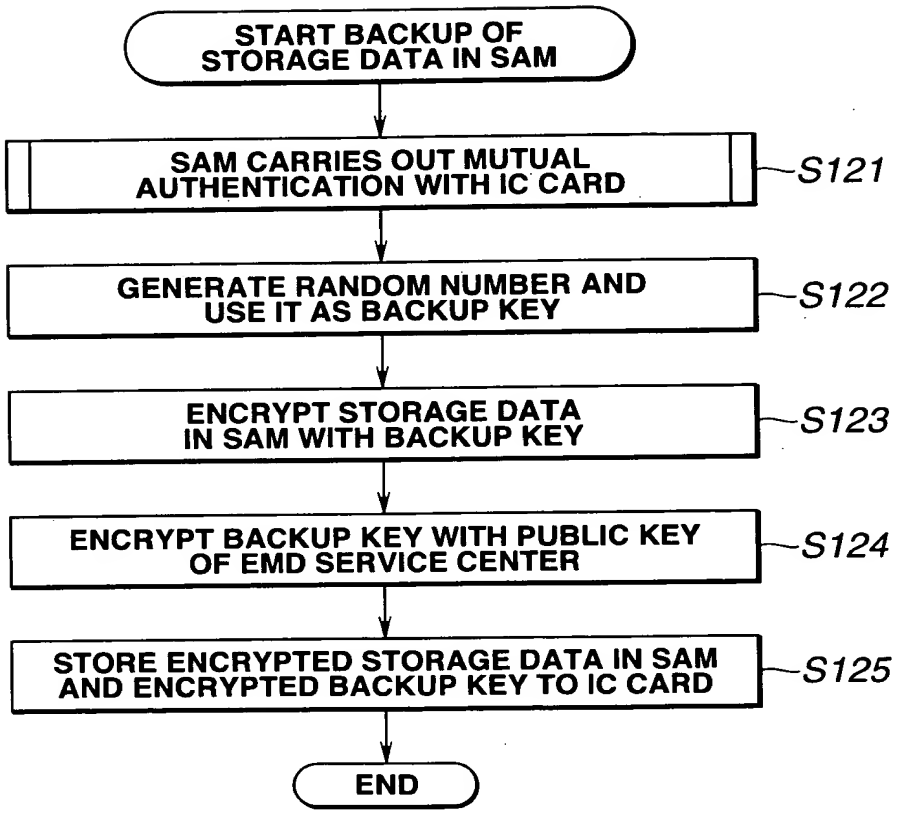
START BACKUP OF STORAGE DATA IN SAM
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH IC CARD
S121
GENERATE RANDOM NUMBER AND USE IT AS BACKUP KEY
S122
ENCRYPT STORAGE DATA IN SAM WITH BACKUP KEY
S123
ENCRYPT BACKUP KEY WITH PUBLIC KEY OF EMD SERVICE CENTER
S124
STORE ENCRYPTED STORAGE DATA IN SAM AND ENCRYPTED BACKUP KEY TO IC CARD
S125
END

FIG.46

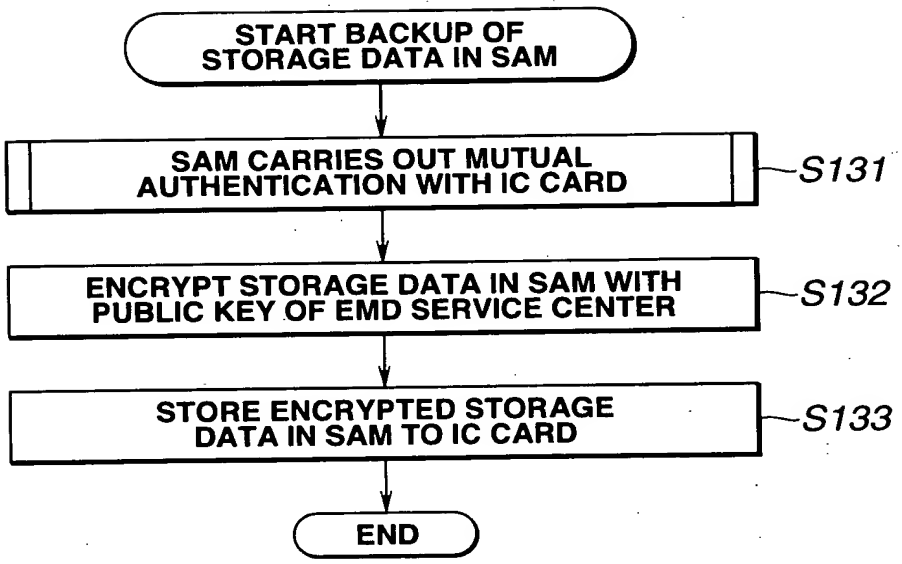
START BACKUP OF STORAGE DATA IN SAM
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH IC CARD
S131
ENCRYPT STORAGE DATA IN SAM WITH PUBLIC KEY OF EMD SERVICE CENTER
S132
STORE ENCRYPTED STORAGE DATA IN SAM TO IC CARD
S133
END

FIG.47

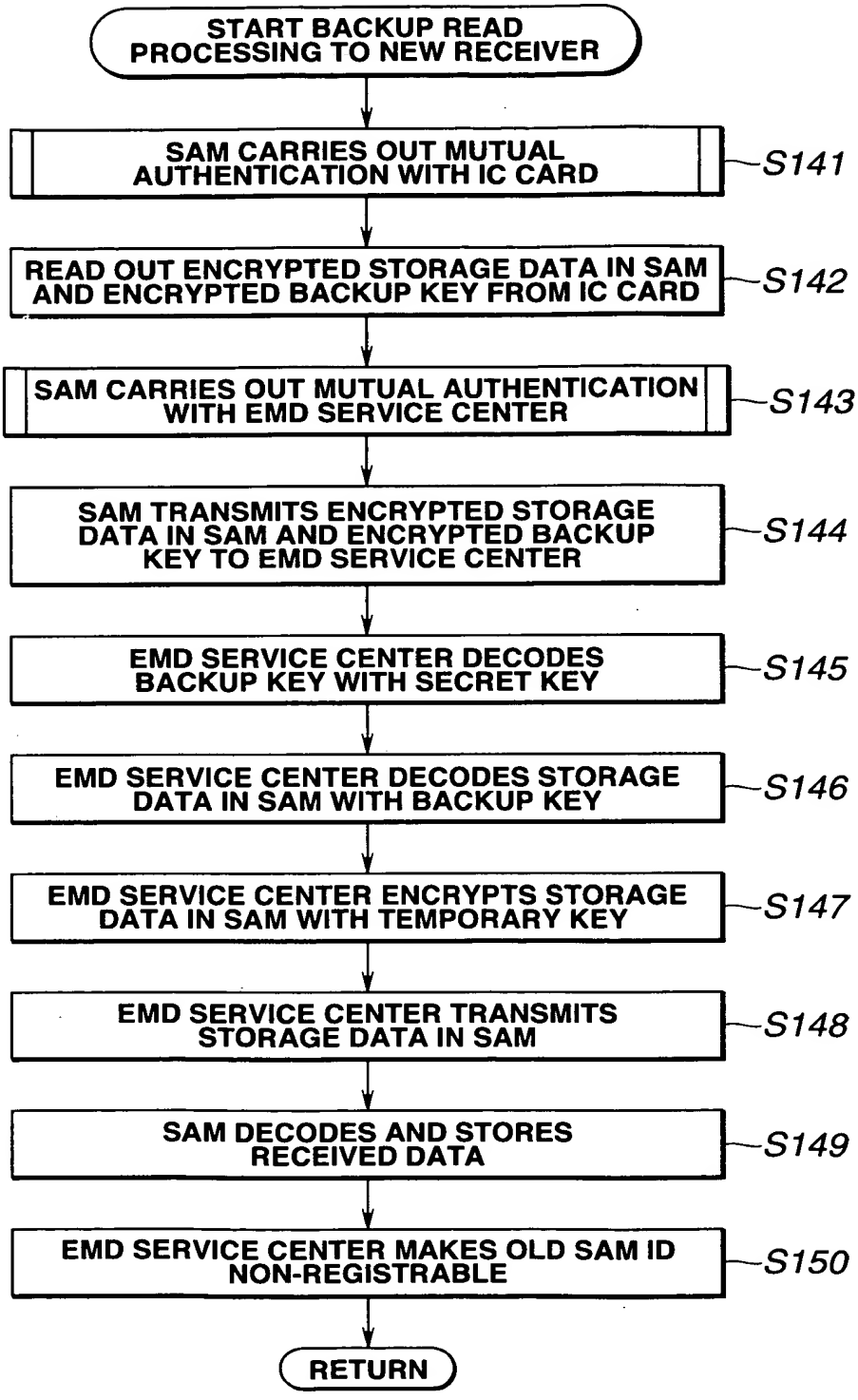
START BACKUP READ PROCESSING TO NEW RECEIVER
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH IC CARD
S141
READ OUT ENCRYPTED STORAGE DATA IN SAM AND ENCRYPTED BACKUP KEY FROM IC CARD
S142
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER
S143
SAM TRANSMITS ENCRYPTED STORAGE DATA IN SAM AND ENCRYPTED BACKUP KEY TO EMD SERVICE CENTER
S144
EMD SERVICE CENTER DECODES BACKUP KEY WITH SECRET KEY
S145
EMD SERVICE CENTER DECODES STORAGE DATA IN SAM WITH BACKUP KEY
S146
EMD SERVICE CENTER ENCRYPTS STORAGE DATA IN SAM WITH TEMPORARY KEY
S147
EMD SERVICE CENTER TRANSMITS STORAGE DATA IN SAM
S148
SAM DECODES AND STORES RECEIVED DATA
S149
EMD SERVICE CENTER MAKES OLD SAM ID NON-REGISTRABLE
S150
RETURN

FIG.48

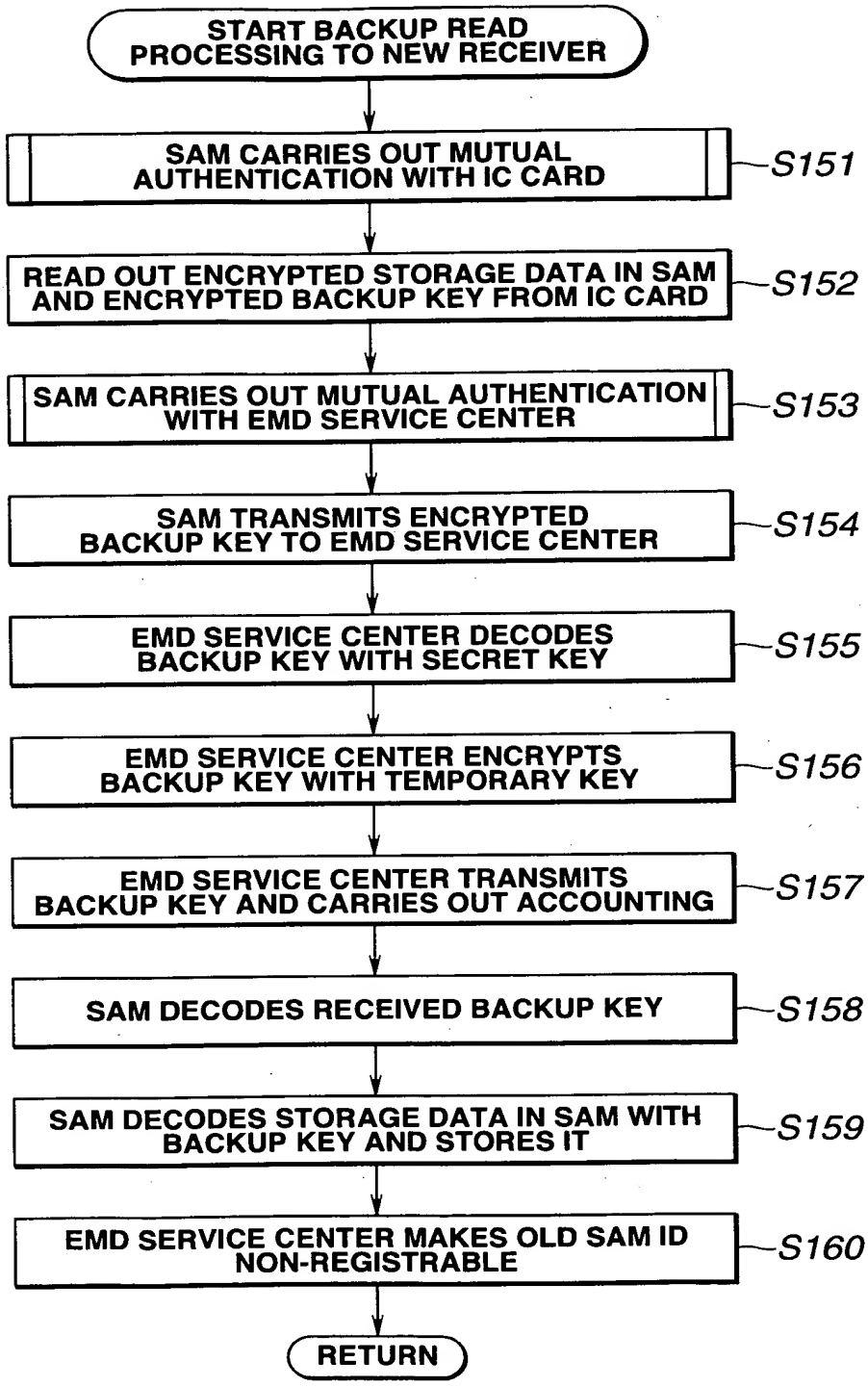
START BACKUP READ PROCESSING TO NEW RECEIVER
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH IC CARD
S151
READ OUT ENCRYPTED STORAGE DATA IN SAM AND ENCRYPTED BACKUP KEY FROM IC CARD
S152
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER
S153
SAM TRANSMITS ENCRYPTED BACKUP KEY TO EMD SERVICE CENTER
S154
EMD SERVICE CENTER DECODES BACKUP KEY WITH SECRET KEY
S155
EMD SERVICE CENTER ENCRYPTS BACKUP KEY WITH TEMPORARY KEY
S156
EMD SERVICE CENTER TRANSMITS BACKUP KEY AND CARRIES OUT ACCOUNTING
S157
SAM DECODES RECEIVED BACKUP KEY
S158
SAM DECODES STORAGE DATA IN SAM WITH BACKUP KEY AND STORES IT
S159
EMD SERVICE CENTER MAKES OLD SAM ID NON-REGISTRABLE
S160
RETURN

FIG.49

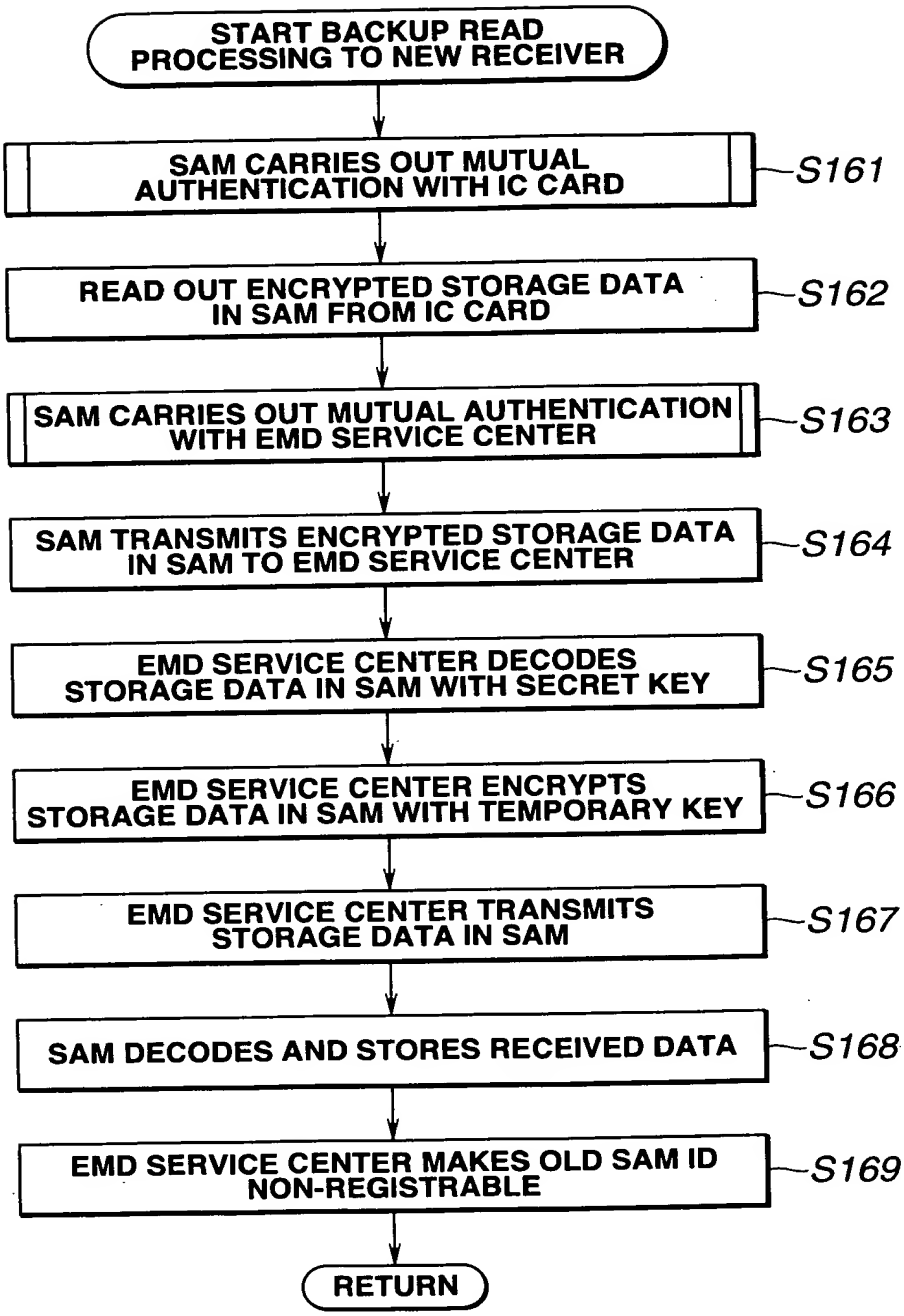
START BACKUP READ PROCESSING TO NEW RECEIVER
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH IC CARD
S161
READ OUT ENCRYPTED STORAGE DATA IN SAM FROM IC CARD
S162
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER
S163
SAM TRANSMITS ENCRYPTED STORAGE DATA IN SAM TO EMD SERVICE CENTER
S164
EMD SERVICE CENTER DECODES STORAGE DATA IN SAM WITH SECRET KEY
S165
EMD SERVICE CENTER ENCRYPTS STORAGE DATA IN SAM WITH TEMPORARY KEY
S166
EMD SERVICE CENTER TRANSMITS STORAGE DATA IN SAM
S167
SAM DECODES AND STORES RECEIVED DATA
S168
EMD SERVICE CENTER MAKES OLD SAM ID NON-REGISTRABLE
S169
RETURN

FIG.50

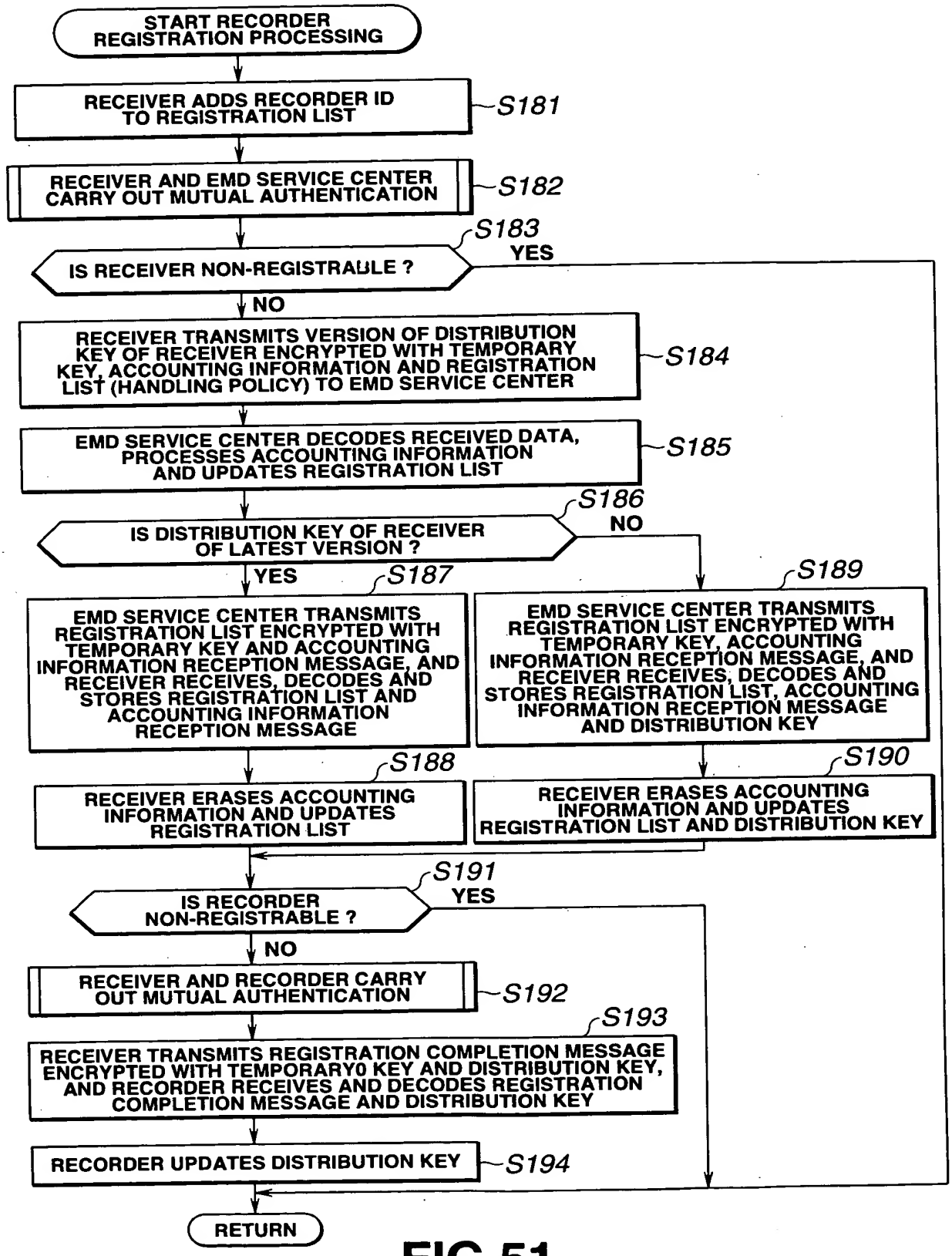
START RECORDER REGISTRATION PROCESSING
RECEIVER ADDS RECORDER ID TO REGISTRATION LIST
S181
RECEIVER AND EMD SERVICE CENTER CARRY OUT MUTUAL AUTHENTICATION
S182
S183
IS RECEIVER NON-REGISTRABLE ?
YES
NO
RECEIVER TRANSMITS VERSION OF DISTRIBUTION KEY OF RECEIVER ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION AND REGISTRATION LIST (HANDLING POLICY) TO EMD SERVICE CENTER
S184
EMD SERVICE CENTER DECODES RECEIVED DATA, PROCESSES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST
S185
S186
IS DISTRIBUTION KEY OF RECEIVER OF LATEST VERSION ?
NO
YES
S187
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY AND ACCOUNTING INFORMATION RECEPTION MESSAGE, AND RECEIVER RECEIVES, DECODES AND STORES REGISTRATION LIST AND ACCOUNTING INFORMATION RECEPTION MESSAGE
S189
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION RECEPTION MESSAGE, AND RECEIVER RECEIVES, DECODES AND STORES REGISTRATION LIST, ACCOUNTING INFORMATION RECEPTION MESSAGE AND DISTRIBUTION KEY
S188
RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST
S190
RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY
S191
IS RECORDER NON-REGISTRABLE ?
YES
NO
RECEIVER AND RECORDER CARRY OUT MUTUAL AUTHENTICATION
S192
S193
RECEIVER TRANSMITS REGISTRATION COMPLETION MESSAGE ENCRYPTED WITH TEMPORARY0 KEY AND DISTRIBUTION KEY, AND RECORDER RECEIVES AND DECODES REGISTRATION COMPLETION MESSAGE AND DISTRIBUTION KEY
RECORDER UPDATES DISTRIBUTION KEY
S194
RETURN

FIG.51

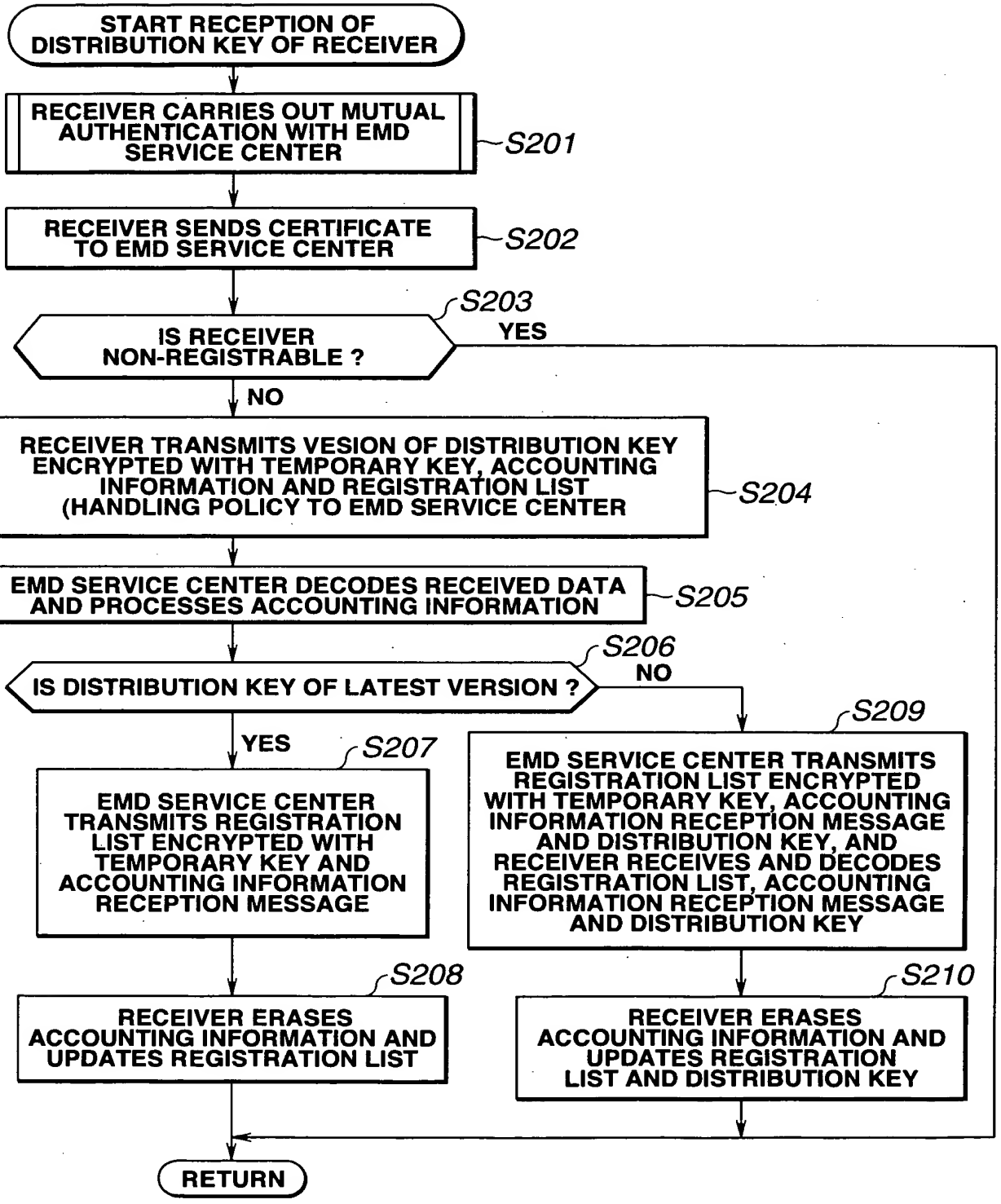
START RECEPTION OF DISTRIBUTION KEY OF RECEIVER
RECEIVER CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CENTER
S201
RECEIVER SENDS CERTIFICATE TO EMD SERVICE CENTER
S202
S203
IS RECEIVER NON-REGISTRABLE ?
YES
NO
RECEIVER TRANSMITS VESION OF DISTRIBUTION KEY ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION AND REGISTRATION LIST (HANDLING POLICY TO EMD SERVICE CENTER
S204
EMD SERVICE CENTER DECODES RECEIVED DATA AND PROCESSES ACCOUNTING INFORMATION
S205
S206
IS DISTRIBUTION KEY OF LATEST VERSION ?
NO
YES
S207
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY AND ACCOUNTING INFORMATION RECEPTION MESSAGE
S209
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY, ACCOUNTING INFORMATION RECEPTION MESSAGE AND DISTRIBUTION KEY, AND RECEIVER RECEIVES AND DECODES REGISTRATION LIST, ACCOUNTING INFORMATION RECEPTION MESSAGE AND DISTRIBUTION KEY
S208
RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST
S210
RECEIVER ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY
RETURN

FIG.52

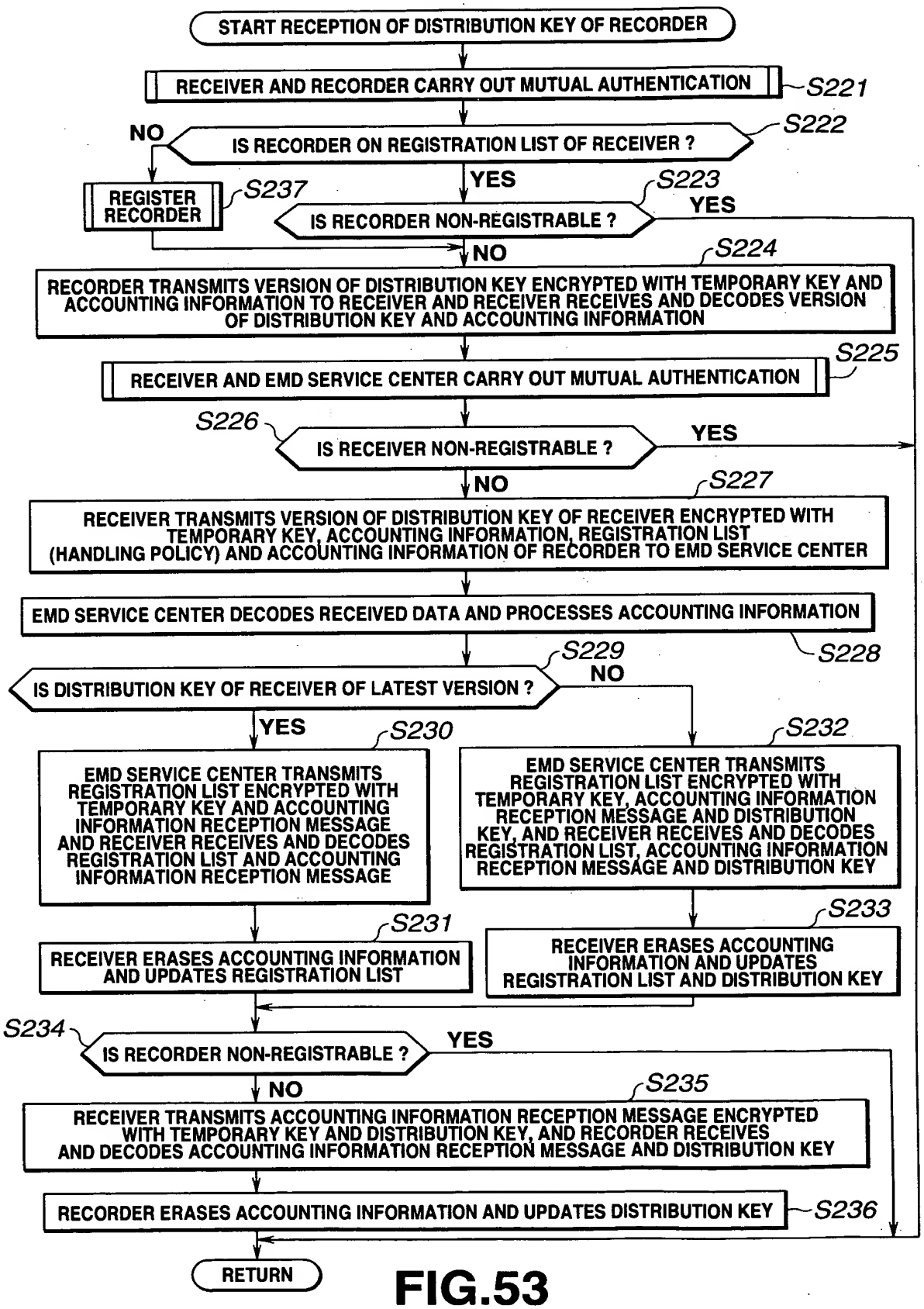

FIG.53

EP 0 863 503 A2

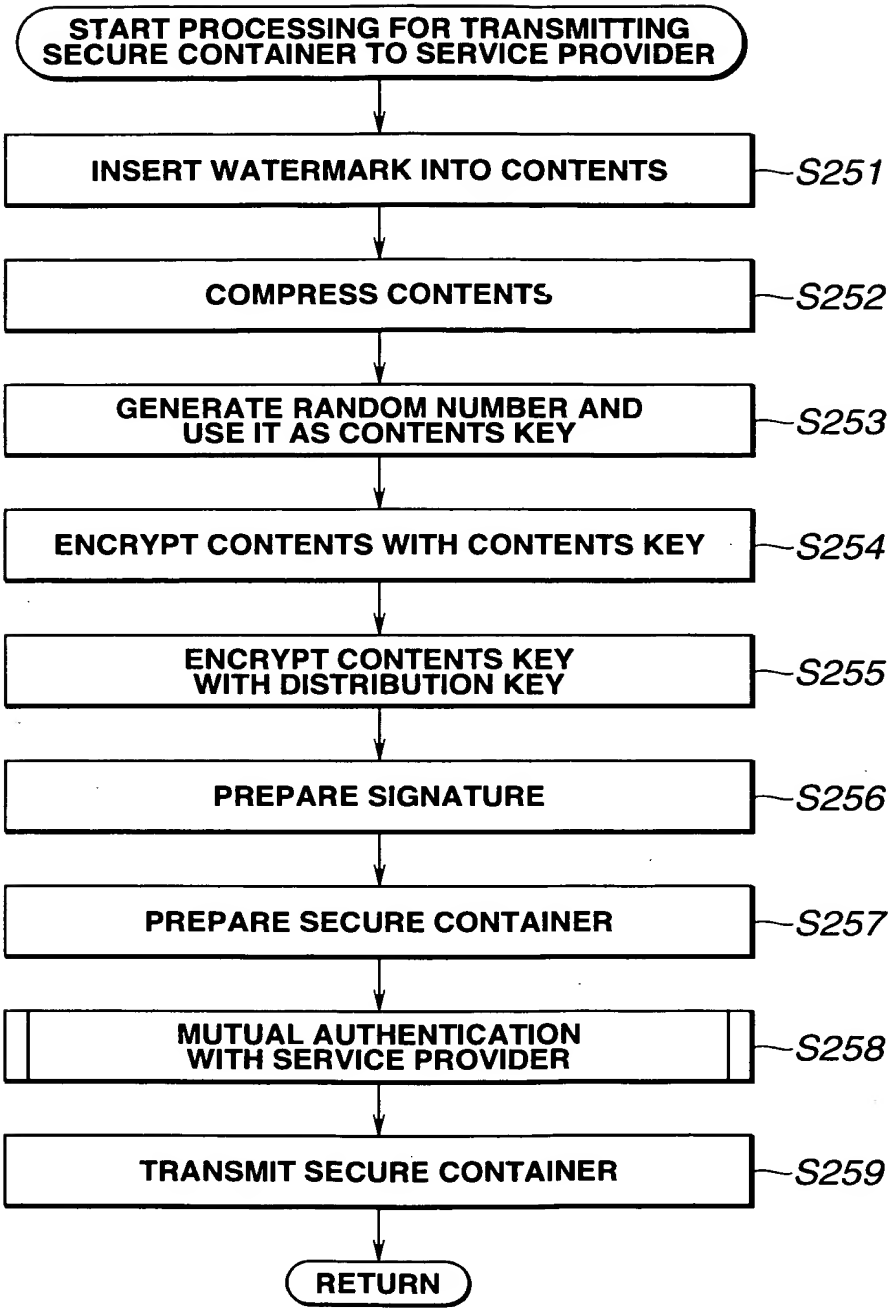

FIG.54

09/501583 - 053004

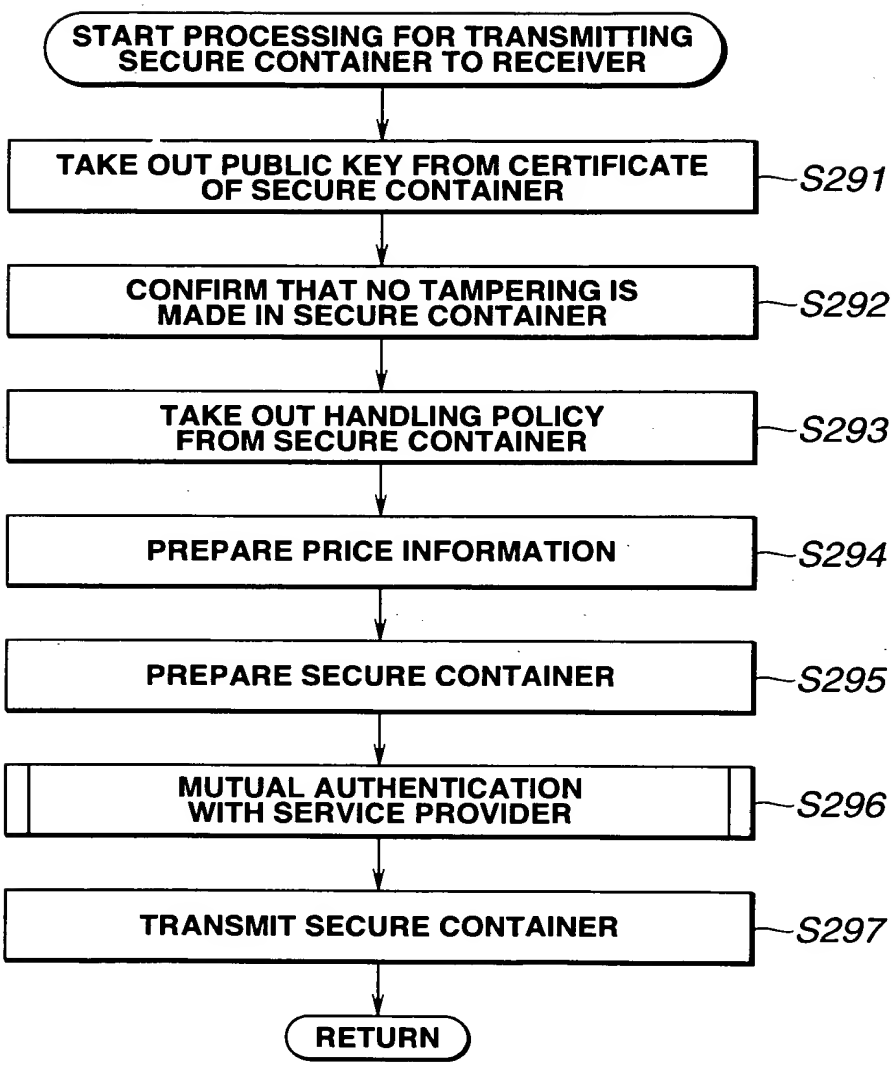
START PROCESSING FOR TRANSMITTING SECURE CONTAINER TO RECEIVER
TAKE OUT PUBLIC KEY FROM CERTIFICATE OF SECURE CONTAINER
S291
CONFIRM THAT NO TAMPERING IS MADE IN SECURE CONTAINER
S292
TAKE OUT HANDLING POLICY FROM SECURE CONTAINER
S293
PREPARE PRICE INFORMATION
S294
PREPARE SECURE CONTAINER
S295
MUTUAL AUTHENTICATION WITH SERVICE PROVIDER
S296
TRANSMIT SECURE CONTAINER
S297
RETURN

FIG.55

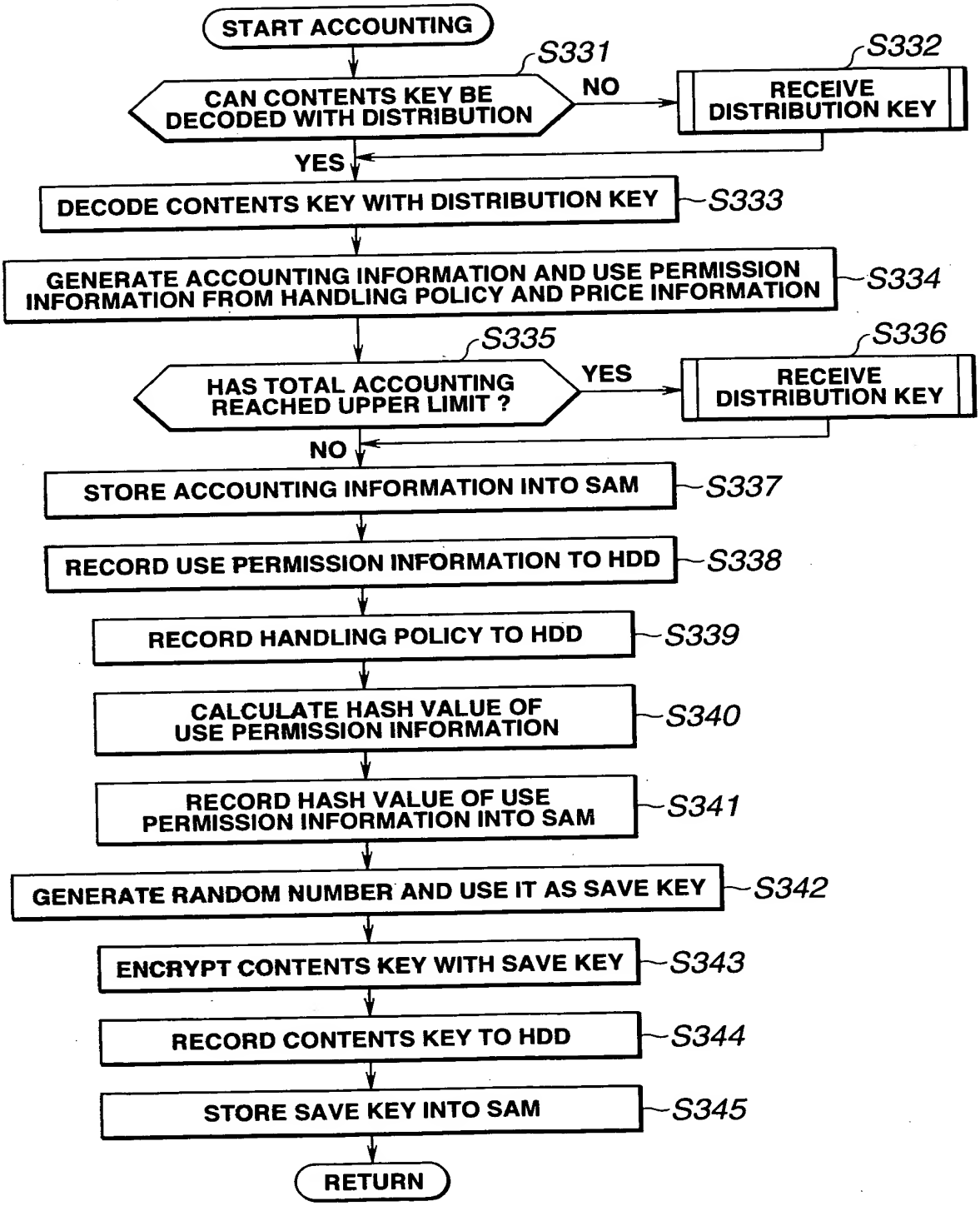
START ACCOUNTING
S331
CAN CONTENTS KEY BE DECODED WITH DISTRIBUTION
NO
S332
RECEIVE DISTRIBUTION KEY
YES
DECODE CONTENTS KEY WITH DISTRIBUTION KEY
S333
GENERATE ACCOUNTING INFORMATION AND USE PERMISSION INFORMATION FROM HANDLING POLICY AND PRICE INFORMATION
S334
S335
HAS TOTAL ACCOUNTING REACHED UPPER LIMIT ?
YES
S336
RECEIVE DISTRIBUTION KEY
NO
STORE ACCOUNTING INFORMATION INTO SAM
S337
RECORD USE PERMISSION INFORMATION TO HDD
S338
RECORD HANDLING POLICY TO HDD
S339
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S340
RECORD HASH VALUE OF USE PERMISSION INFORMATION INTO SAM
S341
GENERATE RANDOM NUMBER AND USE IT AS SAVE KEY
S342
ENCRYPT CONTENTS KEY WITH SAVE KEY
S343
RECORD CONTENTS KEY TO HDD
S344
STORE SAVE KEY INTO SAM
S345
RETURN

FIG.56

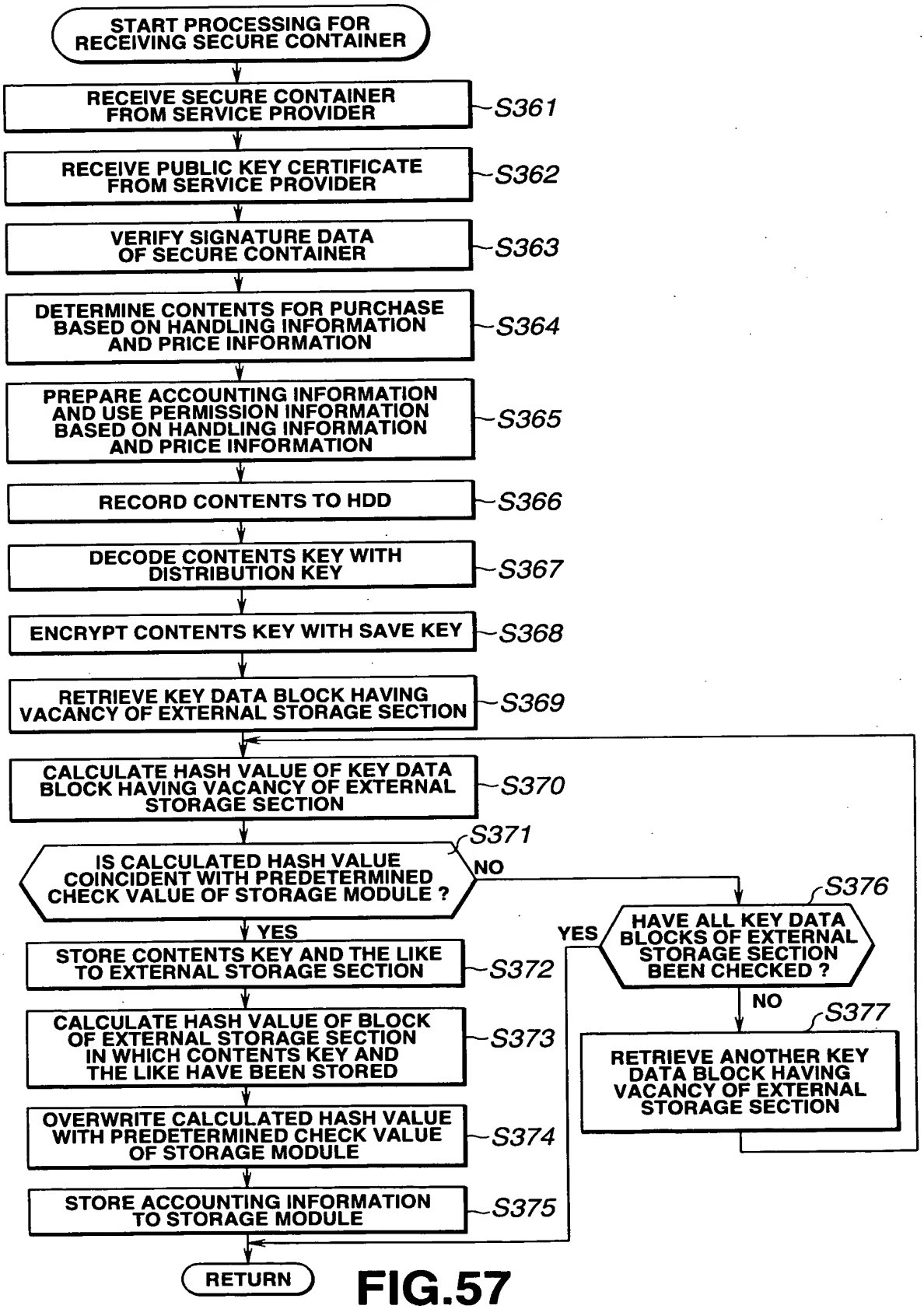
START PROCESSING FOR RECEIVING SECURE CONTAINER
RECEIVE SECURE CONTAINER FROM SERVICE PROVIDER
S361
RECEIVE PUBLIC KEY CERTIFICATE FROM SERVICE PROVIDER
S362
VERIFY SIGNATURE DATA OF SECURE CONTAINER
S363
DETERMINE CONTENTS FOR PURCHASE BASED ON HANDLING INFORMATION AND PRICE INFORMATION
S364
PREPARE ACCOUNTING INFORMATION AND USE PERMISSION INFORMATION BASED ON HANDLING INFORMATION AND PRICE INFORMATION
S365
RECORD CONTENTS TO HDD
S366
DECODE CONTENTS KEY WITH DISTRIBUTION KEY
S367
ENCRYPT CONTENTS KEY WITH SAVE KEY
S368
RETRIEVE KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S369
CALCULATE HASH VALUE OF KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S370
S371
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE ?
NO
YES
S376
HAVE ALL KEY DATA BLOCKS OF EXTERNAL STORAGE SECTION BEEN CHECKED ?
YES
NO
S377
RETRIEVE ANOTHER KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
STORE CONTENTS KEY AND THE LIKE TO EXTERNAL STORAGE SECTION
S372
CALCULATE HASH VALUE OF BLOCK OF EXTERNAL STORAGE SECTION IN WHICH CONTENTS KEY AND THE LIKE HAVE BEEN STORED
S373
OVERWRITE CALCULATED HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE
S374
STORE ACCOUNTING INFORMATION TO STORAGE MODULE
S375
RETURN

FIG.57

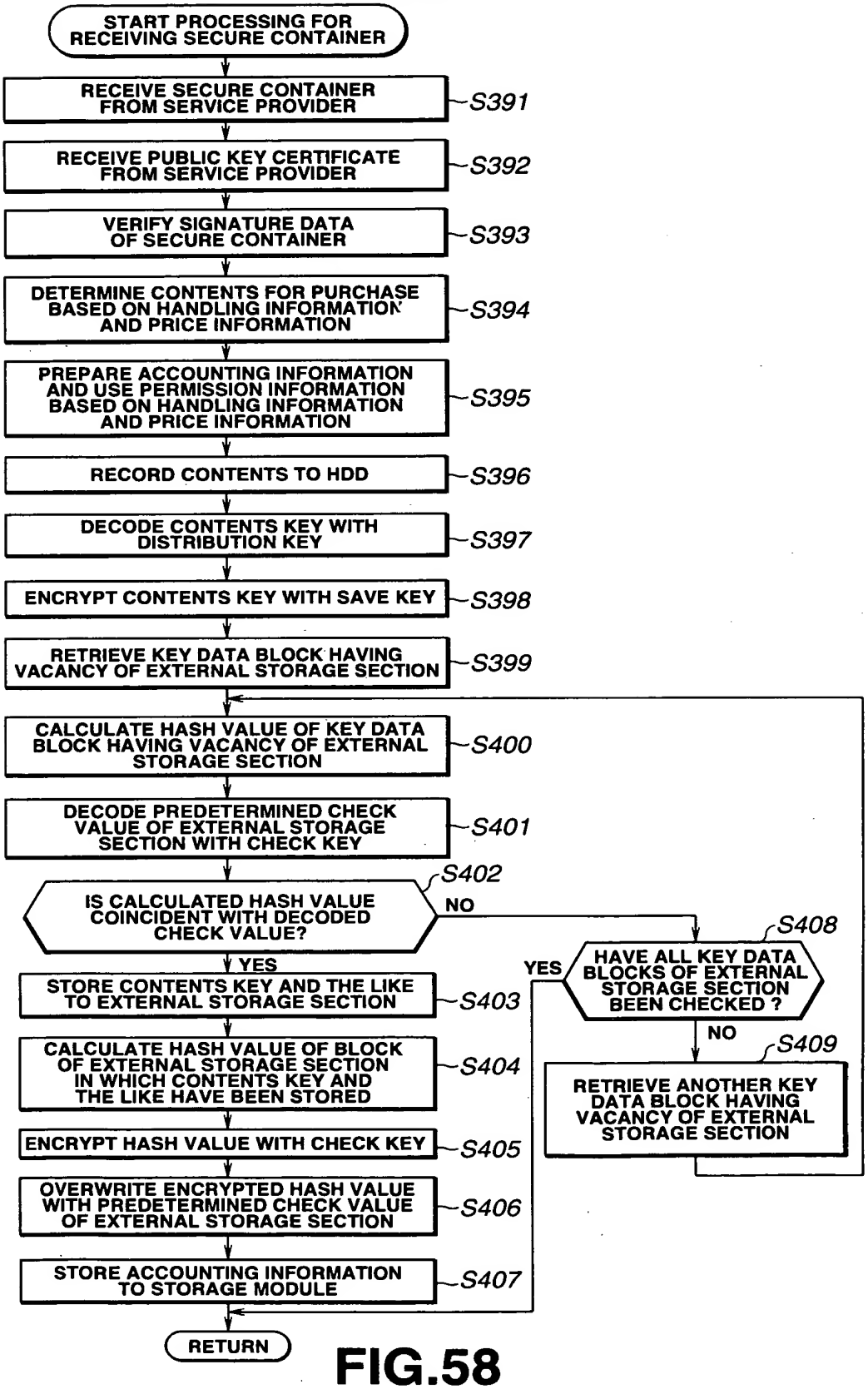
START PROCESSING FOR RECEIVING SECURE CONTAINER
RECEIVE SECURE CONTAINER FROM SERVICE PROVIDER
S391
RECEIVE PUBLIC KEY CERTIFICATE FROM SERVICE PROVIDER
S392
VERIFY SIGNATURE DATA OF SECURE CONTAINER
S393
DETERMINE CONTENTS FOR PURCHASE BASED ON HANDLING INFORMATION AND PRICE INFORMATION
S394
PREPARE ACCOUNTING INFORMATION AND USE PERMISSION INFORMATION BASED ON HANDLING INFORMATION AND PRICE INFORMATION
S395
RECORD CONTENTS TO HDD
S396
DECODE CONTENTS KEY WITH DISTRIBUTION KEY
S397
ENCRYPT CONTENTS KEY WITH SAVE KEY
S398
RETRIEVE KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S399
CALCULATE HASH VALUE OF KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S400
DECODE PREDETERMINED CHECK VALUE OF EXTERNAL STORAGE SECTION WITH CHECK KEY
S401
S402
IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE?
NO
YES
S408
HAVE ALL KEY DATA BLOCKS OF EXTERNAL STORAGE SECTION BEEN CHECKED ?
YES
NO
S409
RETRIEVE ANOTHER KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
STORE CONTENTS KEY AND THE LIKE TO EXTERNAL STORAGE SECTION
S403
CALCULATE HASH VALUE OF BLOCK OF EXTERNAL STORAGE SECTION IN WHICH CONTENTS KEY AND THE LIKE HAVE BEEN STORED
S404
ENCRYPT HASH VALUE WITH CHECK KEY
S405
OVERWRITE ENCRYPTED HASH VALUE WITH PREDETERMINED CHECK VALUE OF EXTERNAL STORAGE SECTION
S406
STORE ACCOUNTING INFORMATION TO STORAGE MODULE
S407
RETURN

FIG.58

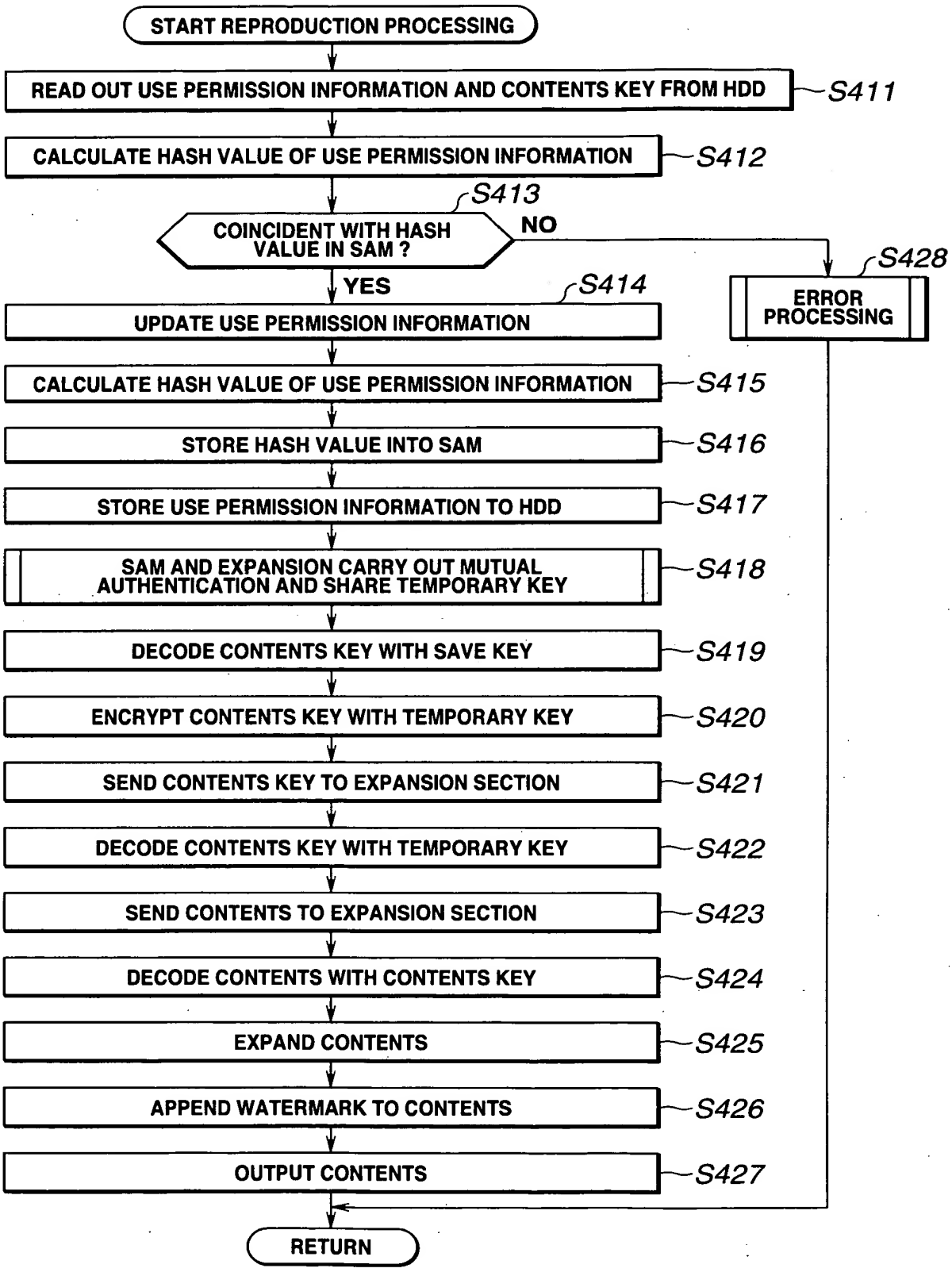

FIG.59

09/581583 06/06/2006 15:58:50

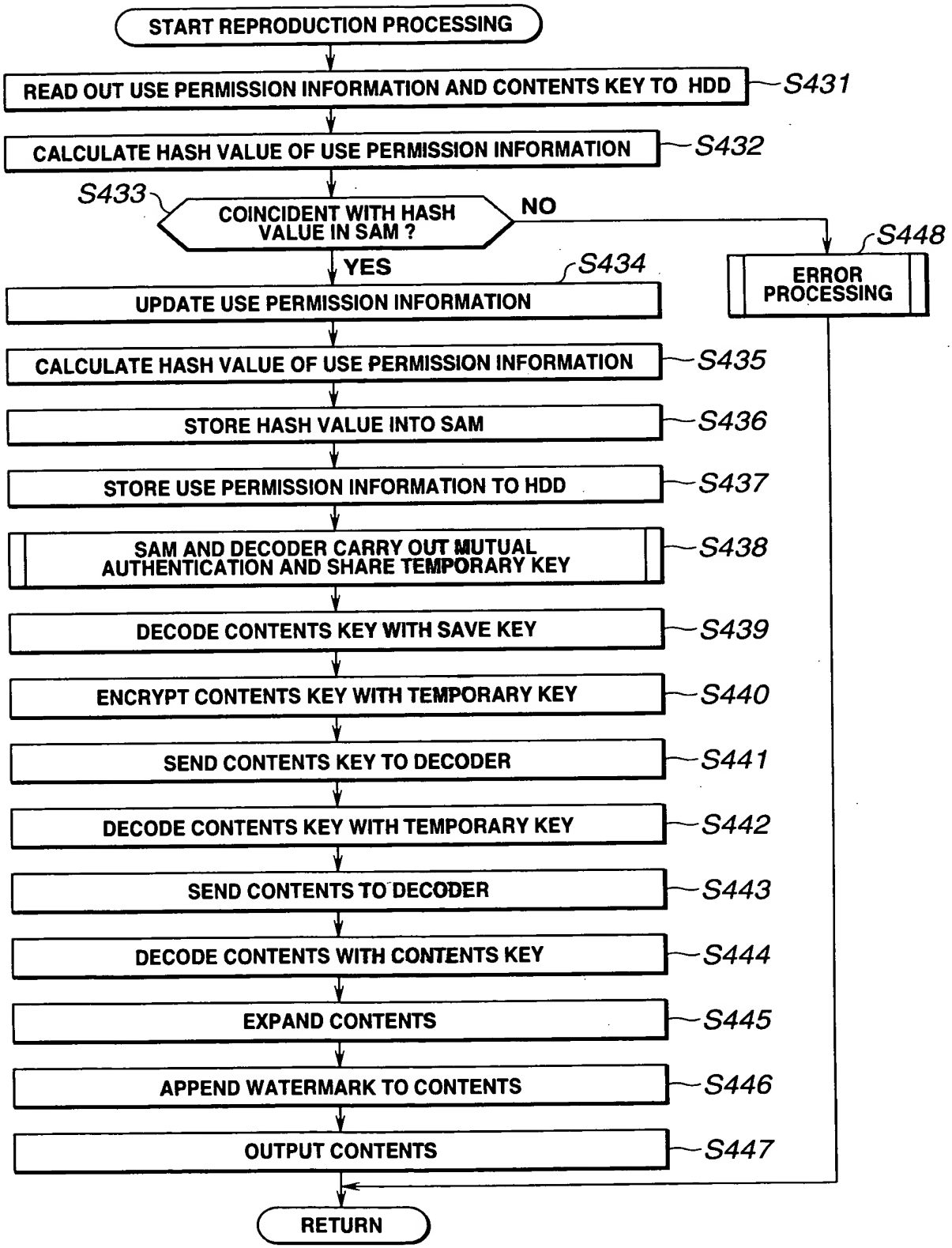
START REPRODUCTION PROCESSING
READ OUT USE PERMISSION INFORMATION AND CONTENTS KEY TO HDD
S431
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S432
S433
COINCIDENT WITH HASH VALUE IN SAM ?
NO
S448
ERROR PROCESSING
YES
S434
UPDATE USE PERMISSION INFORMATION
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S435
STORE HASH VALUE INTO SAM
S436
STORE USE PERMISSION INFORMATION TO HDD
S437
SAM AND DECODER CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S438
DECODE CONTENTS KEY WITH SAVE KEY
S439
ENCRYPT CONTENTS KEY WITH TEMPORARY KEY
S440
SEND CONTENTS KEY TO DECODER
S441
DECODE CONTENTS KEY WITH TEMPORARY KEY
S442
SEND CONTENTS TO DECODER
S443
DECODE CONTENTS WITH CONTENTS KEY
S444
EXPAND CONTENTS
S445
APPEND WATERMARK TO CONTENTS
S446
OUTPUT CONTENTS
S447
RETURN

FIG.60

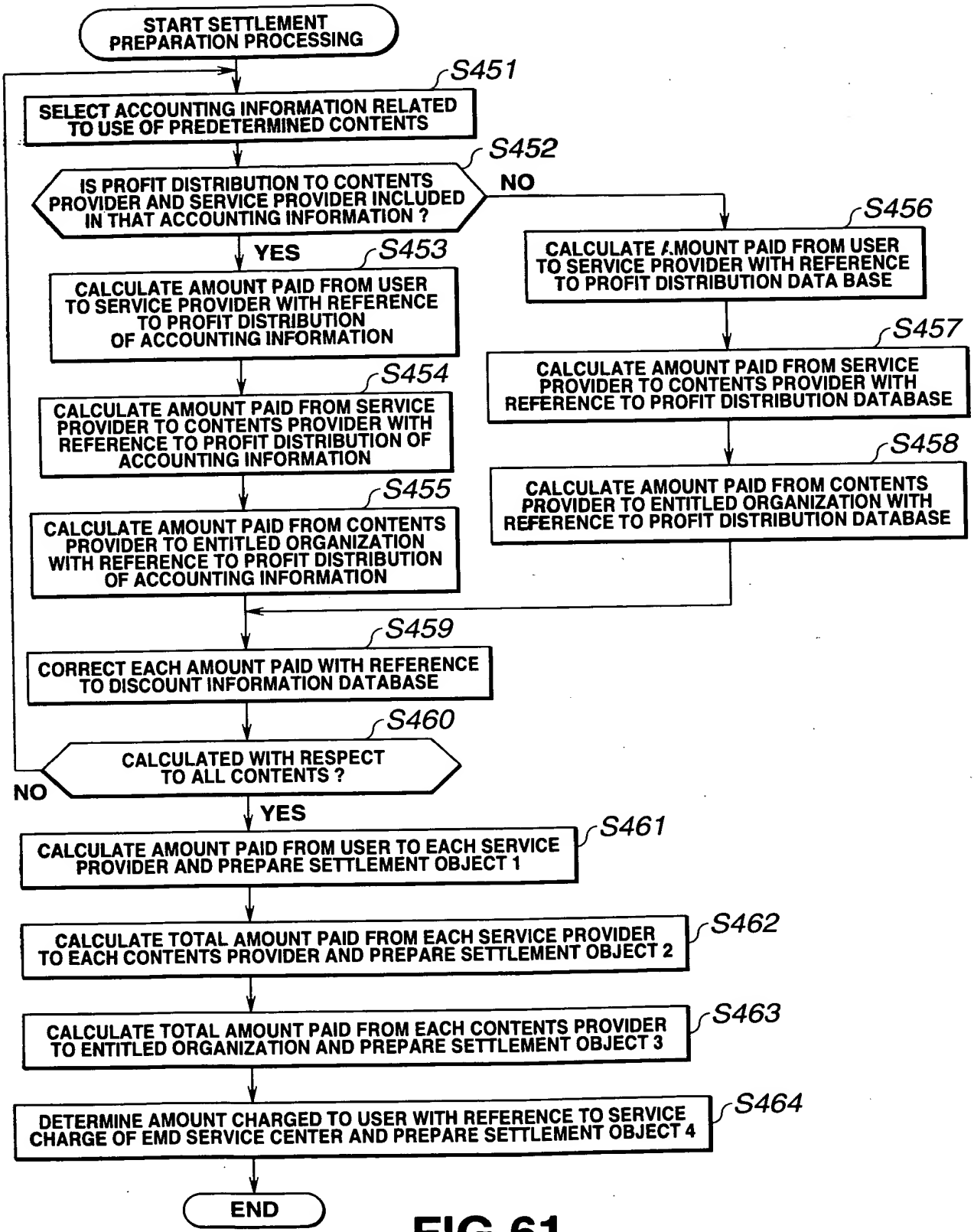
START SETTLEMENT PREPARATION PROCESSING
S451
SELECT ACCOUNTING INFORMATION RELATED TO USE OF PREDETERMINED CONTENTS
S452
IS PROFIT DISTRIBUTION TO CONTENTS PROVIDER AND SERVICE PROVIDER INCLUDED IN THAT ACCOUNTING INFORMATION ?
NO
YES
S453
CALCULATE AMOUNT PAID FROM USER TO SERVICE PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF ACCOUNTING INFORMATION
S454
CALCULATE AMOUNT PAID FROM SERVICE PROVIDER TO CONTENTS PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION OF ACCOUNTING INFORMATION
S455
CALCULATE AMOUNT PAID FROM CONTENTS PROVIDER TO ENTITLED ORGANIZATION WITH REFERENCE TO PROFIT DISTRIBUTION OF ACCOUNTING INFORMATION
S456
CALCULATE AMOUNT PAID FROM USER TO SERVICE PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION DATA BASE
S457
CALCULATE AMOUNT PAID FROM SERVICE PROVIDER TO CONTENTS PROVIDER WITH REFERENCE TO PROFIT DISTRIBUTION DATABASE
S458
CALCULATE AMOUNT PAID FROM CONTENTS PROVIDER TO ENTITLED ORGANIZATION WITH REFERENCE TO PROFIT DISTRIBUTION DATABASE
S459
CORRECT EACH AMOUNT PAID WITH REFERENCE TO DISCOUNT INFORMATION DATABASE
S460
CALCULATED WITH RESPECT TO ALL CONTENTS ?
NO
YES
S461
CALCULATE AMOUNT PAID FROM USER TO EACH SERVICE PROVIDER AND PREPARE SETTLEMENT OBJECT 1
S462
CALCULATE TOTAL AMOUNT PAID FROM EACH SERVICE PROVIDER TO EACH CONTENTS PROVIDER AND PREPARE SETTLEMENT OBJECT 2
S463
CALCULATE TOTAL AMOUNT PAID FROM EACH CONTENTS PROVIDER TO ENTITLED ORGANIZATION AND PREPARE SETTLEMENT OBJECT 3
S464
DETERMINE AMOUNT CHARGED TO USER WITH REFERENCE TO SERVICE CHARGE OF EMD SERVICE CENTER AND PREPARE SETTLEMENT OBJECT 4
END

FIG.61

FIG.62A

CREDIT SETTLEMENT
OBJECT 1

PAYER : USER ID
AMOUNT CHARGED : x
PAYEE : SERVICE PROVIDER ID
AMOUNT PAID : x1

FIG.62B

CREDIT SETTLEMENT
OBJECT 2

PAYER : CREDIT SETTLEMENT OBJECT 1
AMOUNT CHARGED : –
PAYEE : CONTENTS PROVIDER ID
AMOUNT PAID : x2

FIG.62C

CREDIT SETTLEMENT
OBJECT 3

PAYER : CREDIT SETTLEMENT OBJECT 1
AMOUNT CHARGED : –
PAYEE : ENTITLED ORGANIZATION ID
AMOUNT PAID : x3

FIG.62D

CREDIT SETTLEMENT
OBJECT 4

PAYER : CREDIT SETTLEMENT OBJECT 1
AMOUNT CHARGED : –
PAYEE : EMD SERVICE CENTER ID
AMOUNT PAID : x4

0957058 - 0957058

FIG.63A

BANK SETTLEMENT
OBJECT 1

PAYER : SERVICE PROVIDER ID
AMOUNT CHARGED : y1
PAYEE : EMD SERVICE CENTER ID
AMOUNT PAID : y1

FIG.63B

BANK SETTLEMENT
OBJECT 2

PAYER : CONTENTS PROVIDER ID
AMOUNT CHARGED : y2
PAYEE : EMD SERVICE CENTER ID
AMOUNT PAID : y2

FIG.63C

BANK SETTLEMENT
OBJECT 3

PAYER : ENTITLED ORGANIZATION ID
AMOUNT CHARGED : y3
PAYEE : EMD SERVICE CENTER ID
AMOUNT PAID : y3

0076050.0050

FIG.64A

CREDIT SETTLEMENT
OBJECT 1

PAYER : USER ID
AMOUNT CHARGED : x
PAYEE : SERVICE PROVIDER ID
AMOUNT PAID : x1

FIG.64B

BANK SETTLEMENT
OBJECT 2

PAYER : SERVICE PROVIDER ID
AMOUNT CHARGED : x2+x3
PAYEE : CONTENTS PROVIDER ID
AMOUNT PAID : x2+x3

FIG.64C

BANK SETTLEMENT
OBJECT 3

PAYER : CONTENTS PROVIDER ID
AMOUNT CHARGED : x3
PAYEE : ENTITLED ORGANIZATION ID
AMOUNT PAID : x3

FIG.64D

CREDIT SETTLEMENT
OBJECT 4

PAYER : CREDIT SETTLEMENT OBJECT 1
AMOUNT CHARGED : –
PAYEE : EMD SERVICE CENTER ID
AMOUNT PAID : x4

0507040-0050

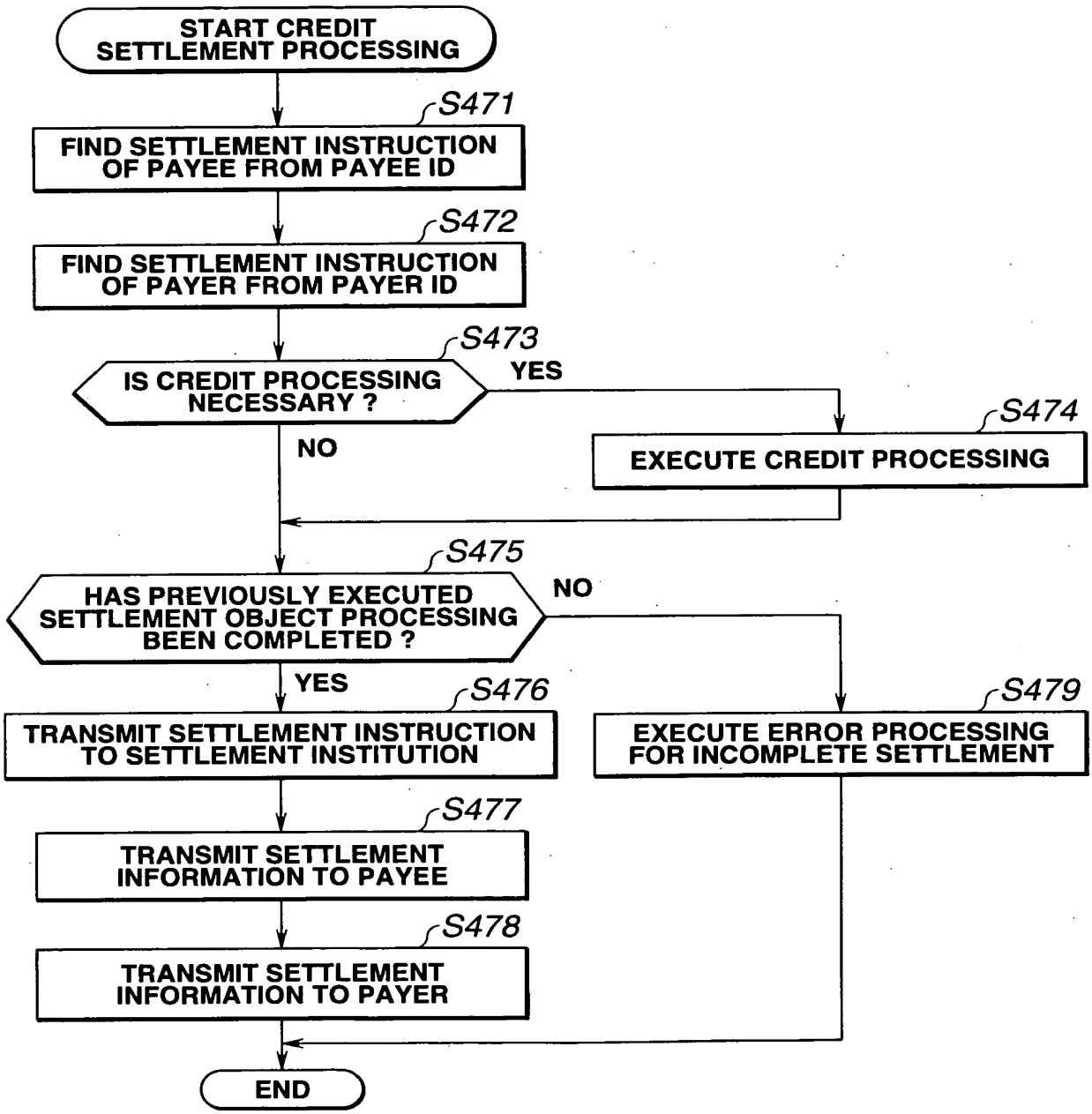
START CREDIT SETTLEMENT PROCESSING
S471
FIND SETTLEMENT INSTRUCTION OF PAYEE FROM PAYEE ID
S472
FIND SETTLEMENT INSTRUCTION OF PAYER FROM PAYER ID
S473
IS CREDIT PROCESSING NECESSARY ?
YES
NO
S474
EXECUTE CREDIT PROCESSING
S475
HAS PREVIOUSLY EXECUTED SETTLEMENT OBJECT PROCESSING BEEN COMPLETED ?
NO
YES
S476
TRANSMIT SETTLEMENT INSTRUCTION TO SETTLEMENT INSTITUTION
S479
EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT
S477
TRANSMIT SETTLEMENT INFORMATION TO PAYEE
S478
TRANSMIT SETTLEMENT INFORMATION TO PAYER
END

FIG.65

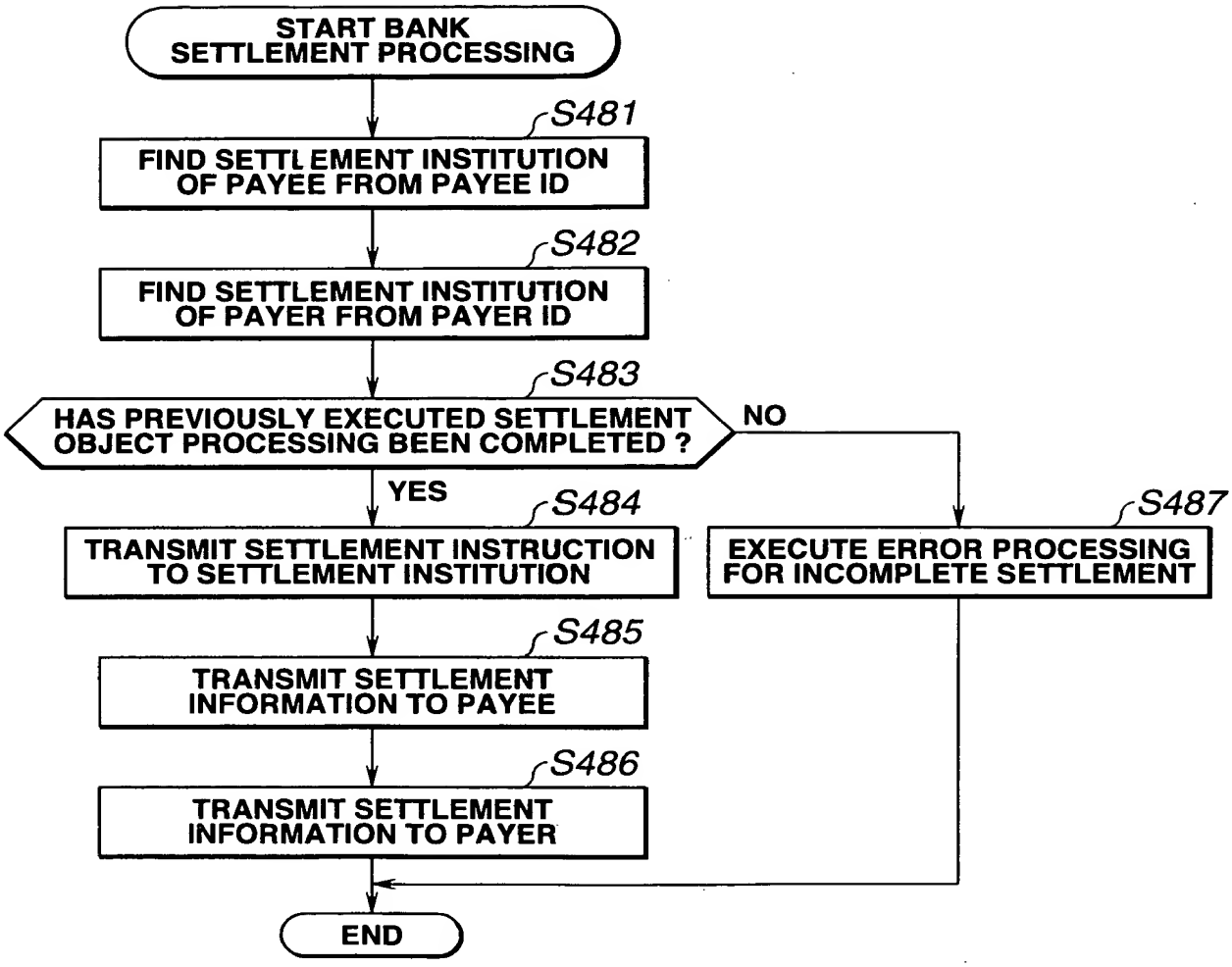
START BANK SETTLEMENT PROCESSING
S481
FIND SETTLEMENT INSTITUTION OF PAYEE FROM PAYEE ID
S482
FIND SETTLEMENT INSTITUTION OF PAYER FROM PAYER ID
S483
HAS PREVIOUSLY EXECUTED SETTLEMENT OBJECT PROCESSING BEEN COMPLETED ?
NO
YES
S484
TRANSMIT SETTLEMENT INSTRUCTION TO SETTLEMENT INSTITUTION
S487
EXECUTE ERROR PROCESSING FOR INCOMPLETE SETTLEMENT
S485
TRANSMIT SETTLEMENT INFORMATION TO PAYEE
S486
TRANSMIT SETTLEMENT INFORMATION TO PAYER
END

FIG.66

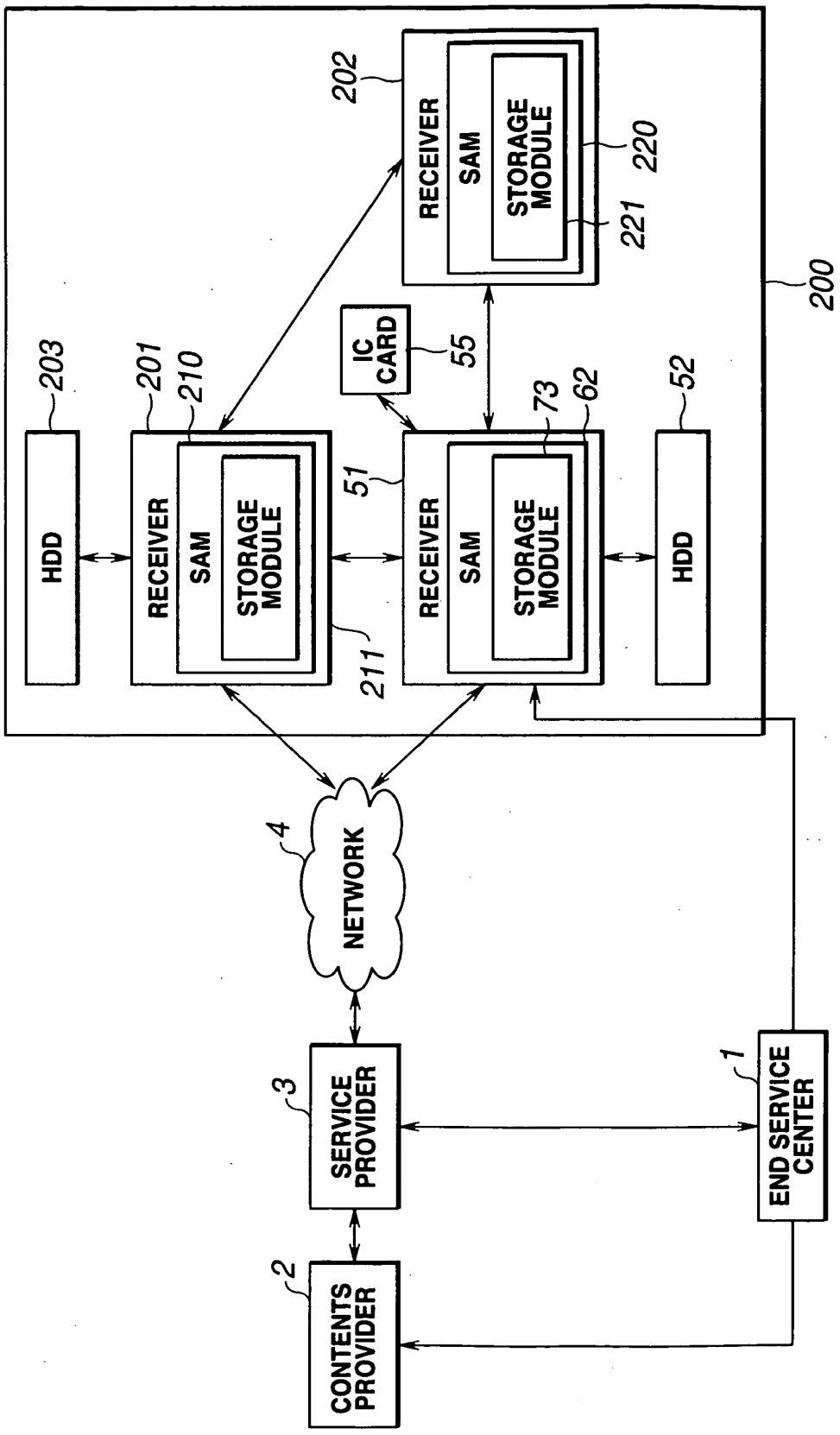
200
202
RECEIVER
SAM
STORAGE MODULE
220
221
IC CARD
55
203
201
210
HDD
RECEIVER
SAM
STORAGE MODULE
51
211
73
62
52
HDD
NETWORK
4
SERVICE PROVIDER
3
END SERVICE CENTER
1
CONTENTS PROVIDER
2

FIG.67

	SAM ID	USER ID	PURCHASE PROCESSING	ACCOUNTING	ACCOUNTING EQUIPMENT	CONTENTS SUPPLY EQUIPMENT	STATUS INFORMATION	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
REGISTRATION CONDITION OF RECEIVER 51	ID OF SAM 62	ID OF USER	AVAILABLE	AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	XXXX
REGISTRATION CONDITION OF RECEIVER 201	ID OF SAM 210	ID OF USER	AVAILABLE	UN-AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	
REGISTRATION CONDITION OF RECEIVER 202	ID OF SAM 220	ID OF USER	UN-AVAILABLE	UN-AVAILABLE	NONE	ID OF SAM 62 ID OF SAM 210	UNLIMITED	XXX	

LIST PART

TARGET SAM ID	ID OF SAM 62
EXPIRATION DATE	XXXX
VERSION NUMBER	XXXX
NUMBER OF EQUIPMENTS CONNECTED	3

TARGET SAM INFORMATION PART

FIG.68

	SAM ID	USER ID	PURCHASE PROCESSING	ACCOUNTING	ACCOUNTING EQUIPMENT	CONTENTS SUPPLY EQUIPMENT	STATUS INFORMATION	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
REGISTRATION CONDITION OF RECEIVER 51	ID OF SAM 62	ID OF USER	AVAILABLE	AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	XXXX
REGISTRATION CONDITION OF RECEIVER 201	ID OF SAM 210	ID OF USER	AVAILABLE	UN-AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	
REGISTRATION CONDITION OF RECEIVER 202	ID OF SAM 220	ID OF USER	UN-AVAILABLE	UN-AVAILABLE	NONE	ID OF SAM 62 ID OF SAM 210	UNLIMITED	XXX	

LIST PART

TARGET SAM ID	ID OF SAM 210
EXPIRATION DATE	XXXX
VERSION NUMBER	XXXX
NUMBER OF EQUIPMENTS CONNECTED	3

TARGET SAM INFORMATION PART

FIG.69

	SAM ID	USER ID	PURCHASE PROCESSING	ACCOUNTING	ACCOUNTING EQUIPMENT	CONTENTS SUPPLY EQUIPMENT	STATUS INFORMATION	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
REGISTRATION CONDITION OF RECEIVER 202	ID OF SAM 220	ID OF USER	UN-AVAILABLE	UN-AVAILABLE	NONE	ID OF SAM 62 ID OF SAM 210	UNLIMITED	XXX	XXXX

LIST PART

TARGET SAM ID	ID OF SAM 220
EXPIRATION DATE	XXXX
VERSION NUMBER	XXXX
NUMBER OF EQUIPMENTS CONNECTED	3

TARGET SAM INFORMATION PART

FIG.70

09/581583

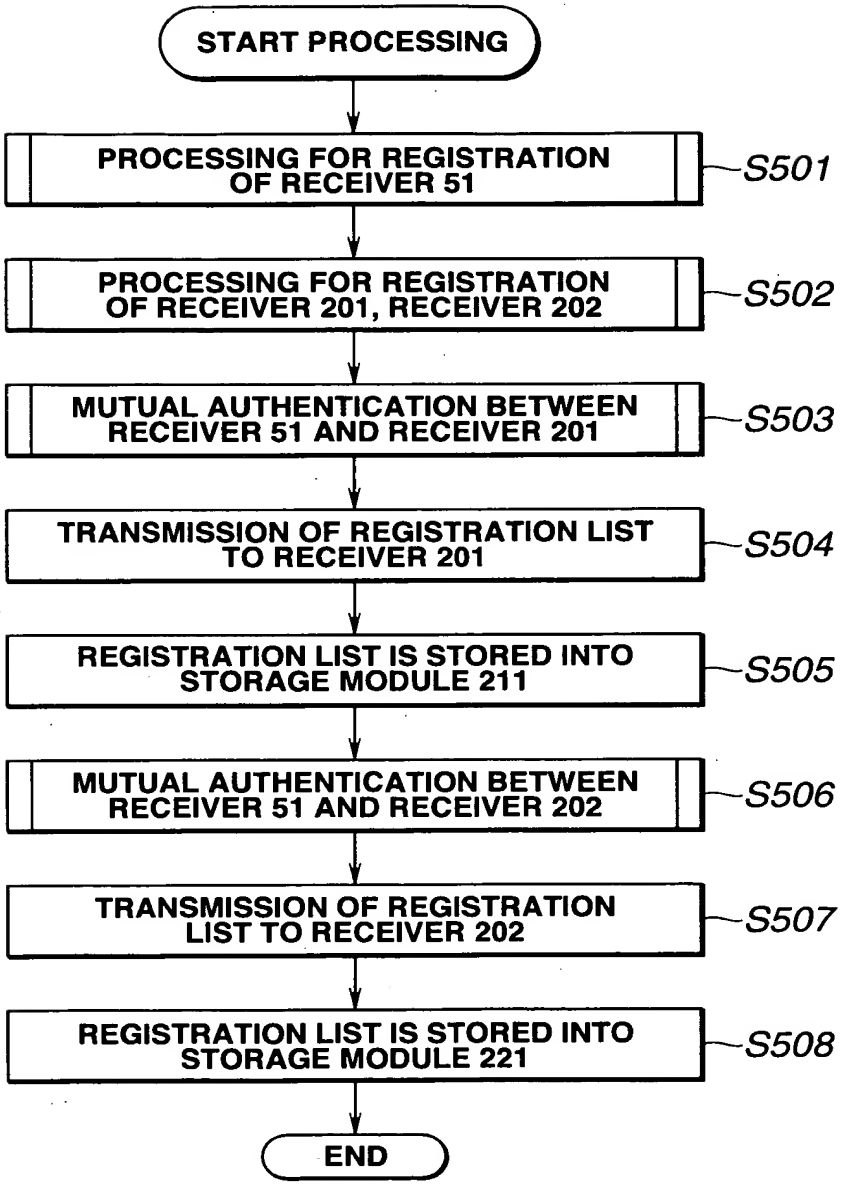
START PROCESSING
PROCESSING FOR REGISTRATION OF RECEIVER 51
S501
PROCESSING FOR REGISTRATION OF RECEIVER 201, RECEIVER 202
S502
MUTUAL AUTHENTICATION BETWEEN RECEIVER 51 AND RECEIVER 201
S503
TRANSMISSION OF REGISTRATION LIST TO RECEIVER 201
S504
REGISTRATION LIST IS STORED INTO STORAGE MODULE 211
S505
MUTUAL AUTHENTICATION BETWEEN RECEIVER 51 AND RECEIVER 202
S506
TRANSMISSION OF REGISTRATION LIST TO RECEIVER 202
S507
REGISTRATION LIST IS STORED INTO STORAGE MODULE 221
S508
END

FIG.71

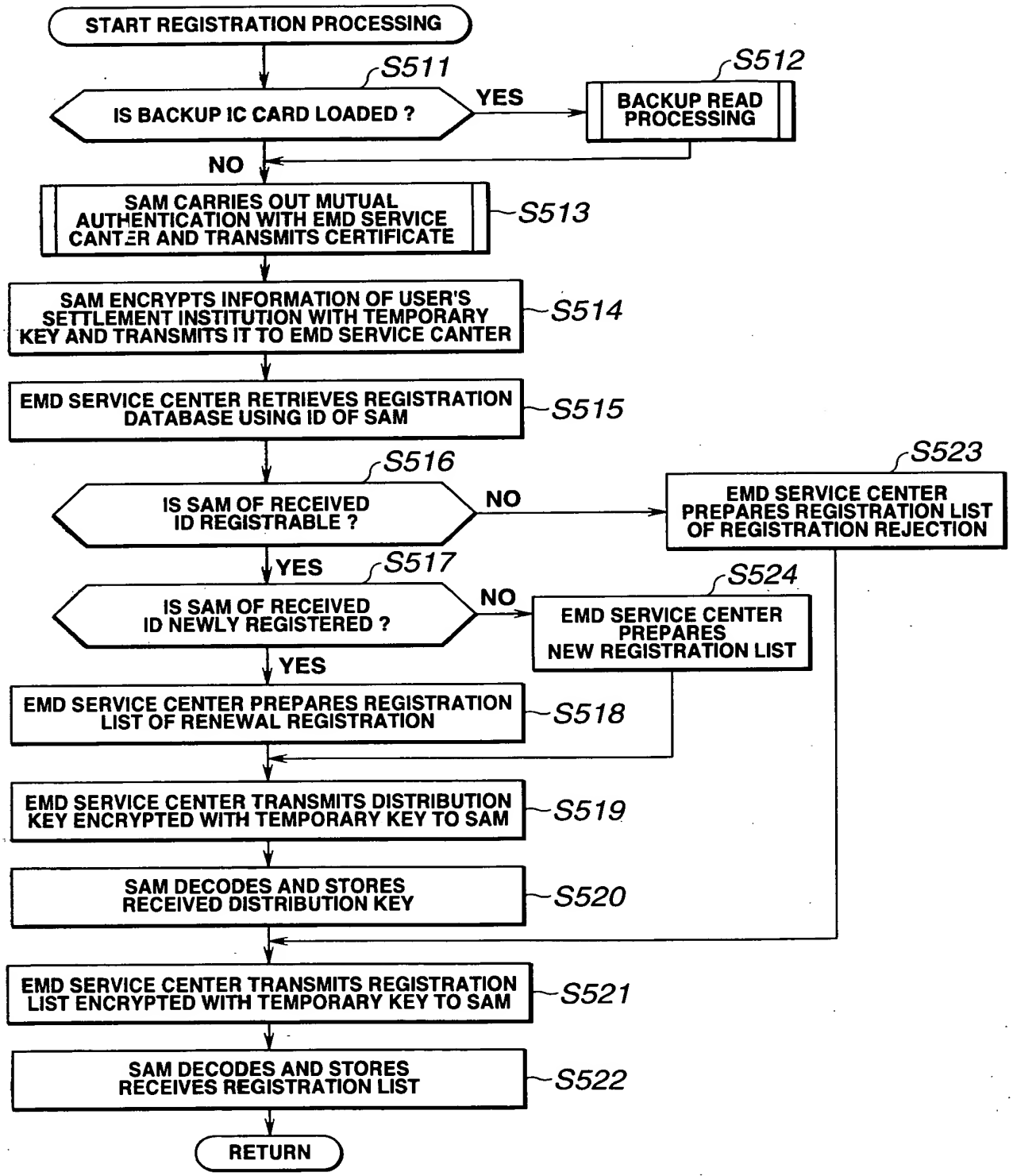
START REGISTRATION PROCESSING
S511
IS BACKUP IC CARD LOADED ?
YES
S512
BACKUP READ PROCESSING
NO
SAM CARRIES OUT MUTUAL AUTHENTICATION WITH EMD SERVICE CANTER AND TRANSMITS CERTIFICATE
S513
SAM ENCRYPTS INFORMATION OF USER'S SETTLEMENT INSTITUTION WITH TEMPORARY KEY AND TRANSMITS IT TO EMD SERVICE CANTER
S514
EMD SERVICE CENTER RETRIEVES REGISTRATION DATABASE USING ID OF SAM
S515
S516
IS SAM OF RECEIVED ID REGISTRABLE ?
NO
S523
EMD SERVICE CENTER PREPARES REGISTRATION LIST OF REGISTRATION REJECTION
YES
S517
IS SAM OF RECEIVED ID NEWLY REGISTERED ?
NO
S524
EMD SERVICE CENTER PREPARES NEW REGISTRATION LIST
YES
EMD SERVICE CENTER PREPARES REGISTRATION LIST OF RENEWAL REGISTRATION
S518
EMD SERVICE CENTER TRANSMITS DISTRIBUTION KEY ENCRYPTED WITH TEMPORARY KEY TO SAM
S519
SAM DECODES AND STORES RECEIVED DISTRIBUTION KEY
S520
EMD SERVICE CENTER TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY TO SAM
S521
SAM DECODES AND STORES RECEIVES REGISTRATION LIST
S522
RETURN

FIG.72

REGISTRATION CONDITION OF RECEIVER 51

SAM ID	USER ID	PURCHASE PROCESSING	ACCOUNTING	ACCOUNTING EQUIPMENT	CONTENTS SUPPLY EQUIPMENT	STATUS INFORMATION	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
ID OF SAM 62	ID OF USER	AVAILABLE	AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	XXXX

} LIST PART

REGISTRATION LIST

TARGET SAM ID	ID OF SAM 62
EXPIRATION DATE	XXXX
VERSION NUMBER	XXXX
NUMBER OF EQUIPMENTS CONNECTED	3

} TARGET SAM INFORMATION PART

FIG.73

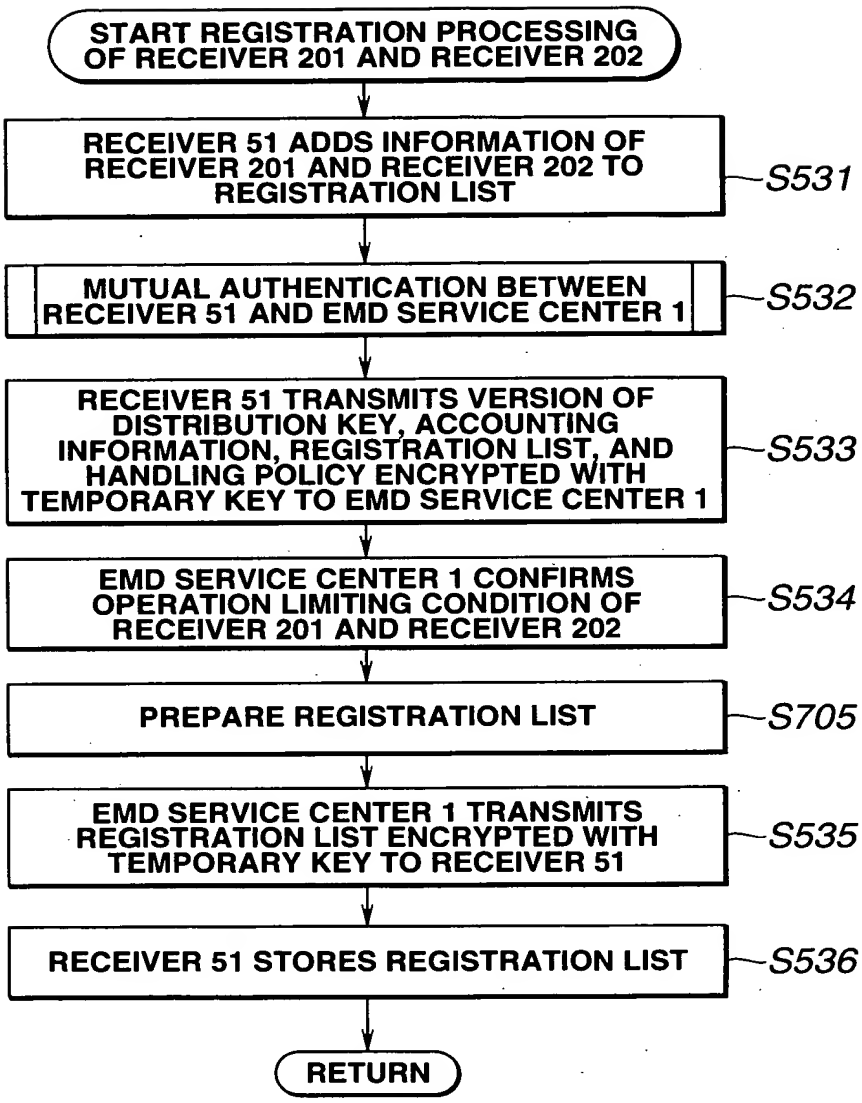
START REGISTRATION PROCESSING OF RECEIVER 201 AND RECEIVER 202
RECEIVER 51 ADDS INFORMATION OF RECEIVER 201 AND RECEIVER 202 TO REGISTRATION LIST
S531
MUTUAL AUTHENTICATION BETWEEN RECEIVER 51 AND EMD SERVICE CENTER 1
S532
RECEIVER 51 TRANSMITS VERSION OF DISTRIBUTION KEY, ACCOUNTING INFORMATION, REGISTRATION LIST, AND HANDLING POLICY ENCRYPTED WITH TEMPORARY KEY TO EMD SERVICE CENTER 1
S533
EMD SERVICE CENTER 1 CONFIRMS OPERATION LIMITING CONDITION OF RECEIVER 201 AND RECEIVER 202
S534
PREPARE REGISTRATION LIST
S705
EMD SERVICE CENTER 1 TRANSMITS REGISTRATION LIST ENCRYPTED WITH TEMPORARY KEY TO RECEIVER 51
S535
RECEIVER 51 STORES REGISTRATION LIST
S536
RETURN

FIG.74

REGISTRATION CONDITION OF RECEIVER 51

SAM ID	USER ID	PURCHASE PROCESSING	ACCOUNTING	ACCOUNTING EQUIPMENT	CONTENTS SUPPLY EQUIPMENT	STATUS INFORMATION	REGISTRATION CONDITION SIGNATURE	REGISTRATION LIST SIGNATURE
ID OF SAM 62	ID OF USER	AVAILABLE	AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	XXXX
ID OF SAM 210		AVAILABLE	UN-AVAILABLE	ID OF SAM 62	NONE	UNLIMITED	XXX	
ID OF SAM 220		UN-AVAILABLE	UN-AVAILABLE	NONE	ID OF SAM 62	UNLIMITED	XXX	
						ID OF SAM 210		

} LIST PART

TARGET SAM ID	ID OF SAM 62
EXPIRATION DATE	XXXX
VERSION NUMBER	XXXX
NUMBER OF EQUIPMENTS CONNECTED	3

} TARGET SAM INFORMATION PART

FIG.75

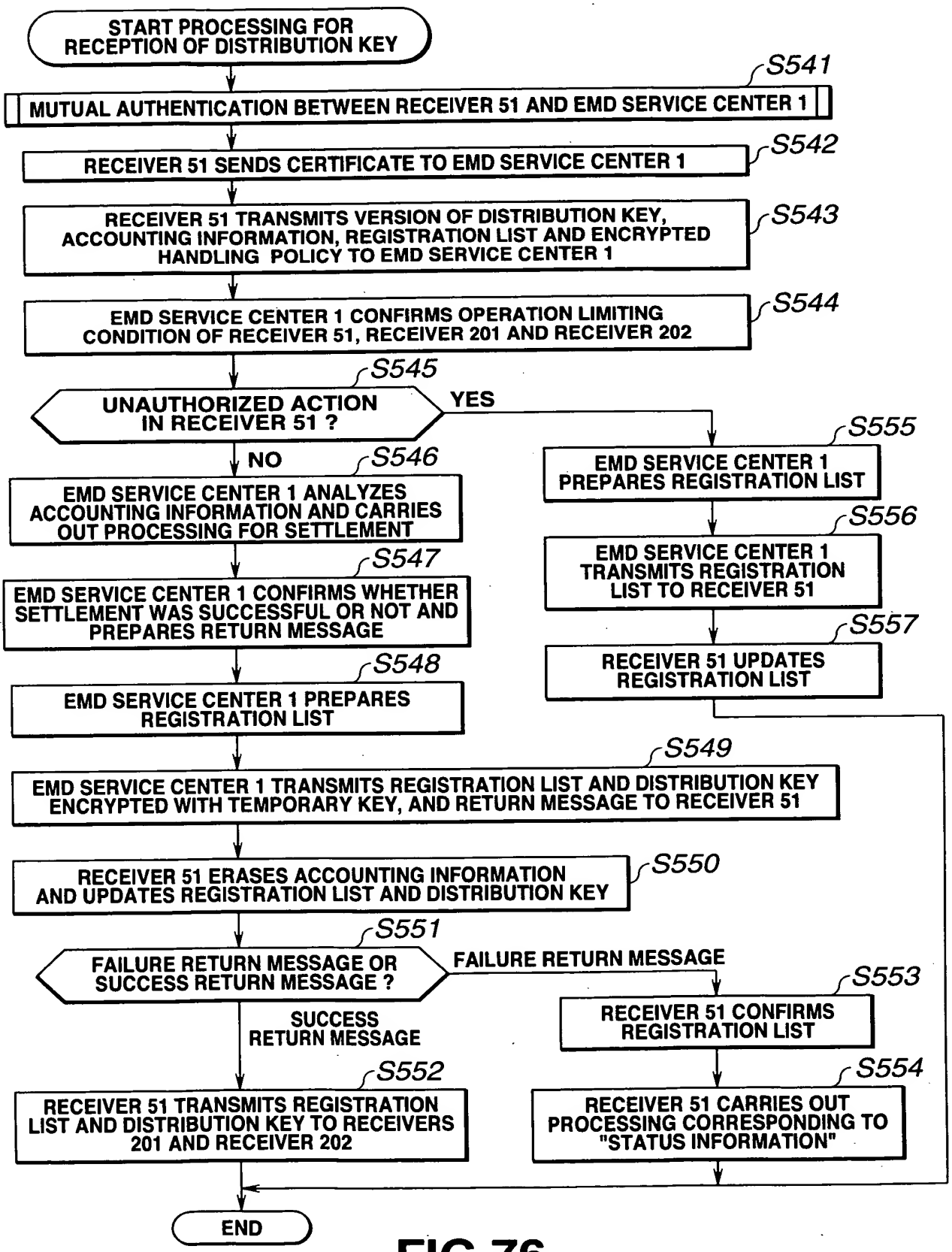
START PROCESSING FOR RECEPTION OF DISTRIBUTION KEY
S541
MUTUAL AUTHENTICATION BETWEEN RECEIVER 51 AND EMD SERVICE CENTER 1
S542
RECEIVER 51 SENDS CERTIFICATE TO EMD SERVICE CENTER 1
S543
RECEIVER 51 TRANSMITS VERSION OF DISTRIBUTION KEY, ACCOUNTING INFORMATION, REGISTRATION LIST AND ENCRYPTED HANDLING POLICY TO EMD SERVICE CENTER 1
S544
EMD SERVICE CENTER 1 CONFIRMS OPERATION LIMITING CONDITION OF RECEIVER 51, RECEIVER 201 AND RECEIVER 202
S545
UNAUTHORIZED ACTION IN RECEIVER 51 ?
YES
NO
S555
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S556
EMD SERVICE CENTER 1 TRANSMITS REGISTRATION LIST TO RECEIVER 51
S557
RECEIVER 51 UPDATES REGISTRATION LIST
S546
EMD SERVICE CENTER 1 ANALYZES ACCOUNTING INFORMATION AND CARRIES OUT PROCESSING FOR SETTLEMENT
S547
EMD SERVICE CENTER 1 CONFIRMS WHETHER SETTLEMENT WAS SUCCESSFUL OR NOT AND PREPARES RETURN MESSAGE
S548
EMD SERVICE CENTER 1 PREPARES REGISTRATION LIST
S549
EMD SERVICE CENTER 1 TRANSMITS REGISTRATION LIST AND DISTRIBUTION KEY ENCRYPTED WITH TEMPORARY KEY, AND RETURN MESSAGE TO RECEIVER 51
S550
RECEIVER 51 ERASES ACCOUNTING INFORMATION AND UPDATES REGISTRATION LIST AND DISTRIBUTION KEY
S551
FAILURE RETURN MESSAGE OR SUCCESS RETURN MESSAGE ?
FAILURE RETURN MESSAGE
S553
RECEIVER 51 CONFIRMS REGISTRATION LIST
SUCCESS RETURN MESSAGE
S552
RECEIVER 51 TRANSMITS REGISTRATION LIST AND DISTRIBUTION KEY TO RECEIVERS 201 AND RECEIVER 202
S554
RECEIVER 51 CARRIES OUT PROCESSING CORRESPONDING TO "STATUS INFORMATION"
END

FIG.76

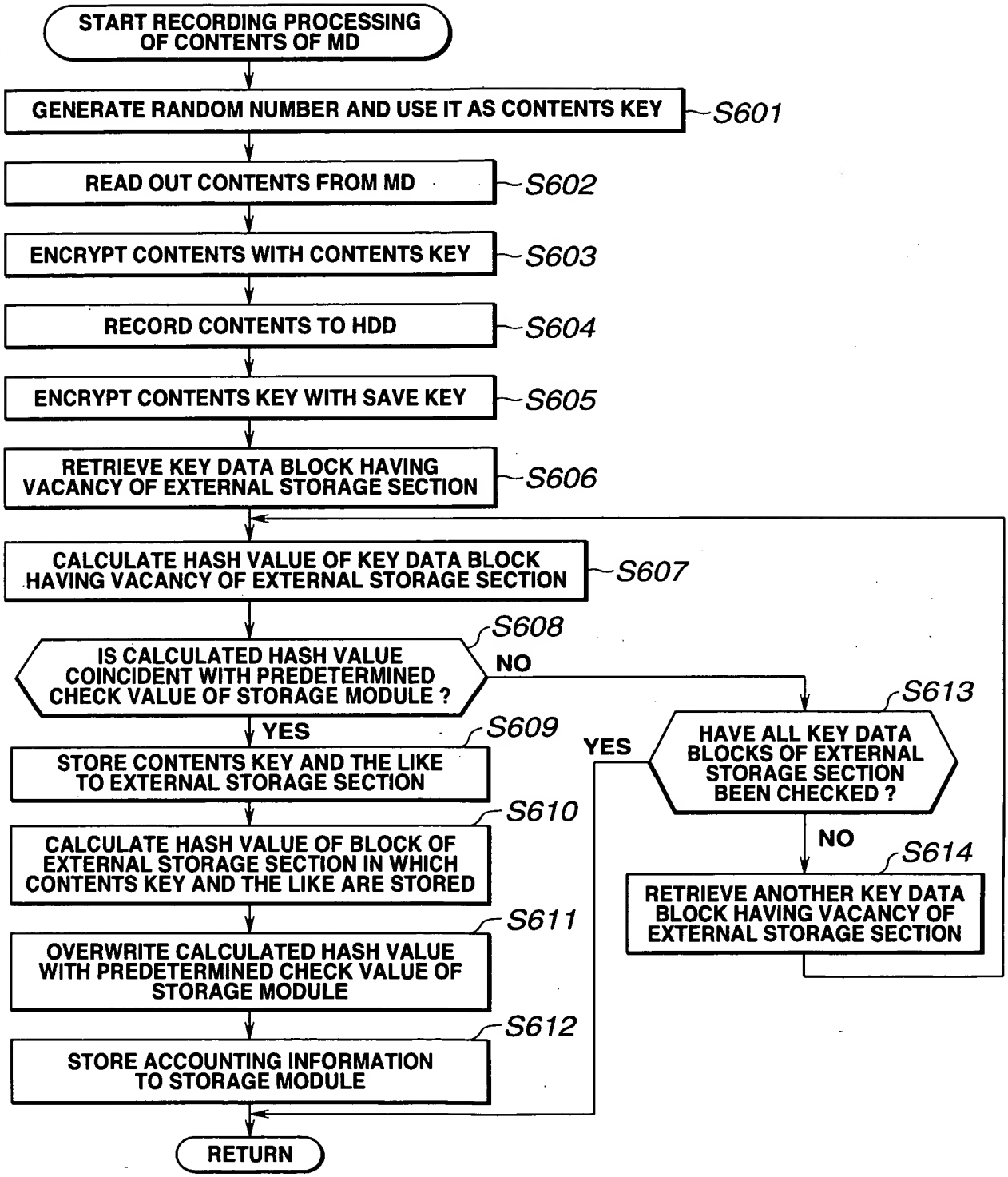
START RECORDING PROCESSING OF CONTENTS OF MD
GENERATE RANDOM NUMBER AND USE IT AS CONTENTS KEY
S601
READ OUT CONTENTS FROM MD
S602
ENCRYPT CONTENTS WITH CONTENTS KEY
S603
RECORD CONTENTS TO HDD
S604
ENCRYPT CONTENTS KEY WITH SAVE KEY
S605
RETRIEVE KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S606
CALCULATE HASH VALUE OF KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S607
S608
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE ?
NO
YES
S609
STORE CONTENTS KEY AND THE LIKE TO EXTERNAL STORAGE SECTION
S610
CALCULATE HASH VALUE OF BLOCK OF EXTERNAL STORAGE SECTION IN WHICH CONTENTS KEY AND THE LIKE ARE STORED
S611
OVERWRITE CALCULATED HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE
S612
STORE ACCOUNTING INFORMATION TO STORAGE MODULE
RETURN
S613
HAVE ALL KEY DATA BLOCKS OF EXTERNAL STORAGE SECTION BEEN CHECKED ?
YES
NO
S614
RETRIEVE ANOTHER KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION

FIG.77

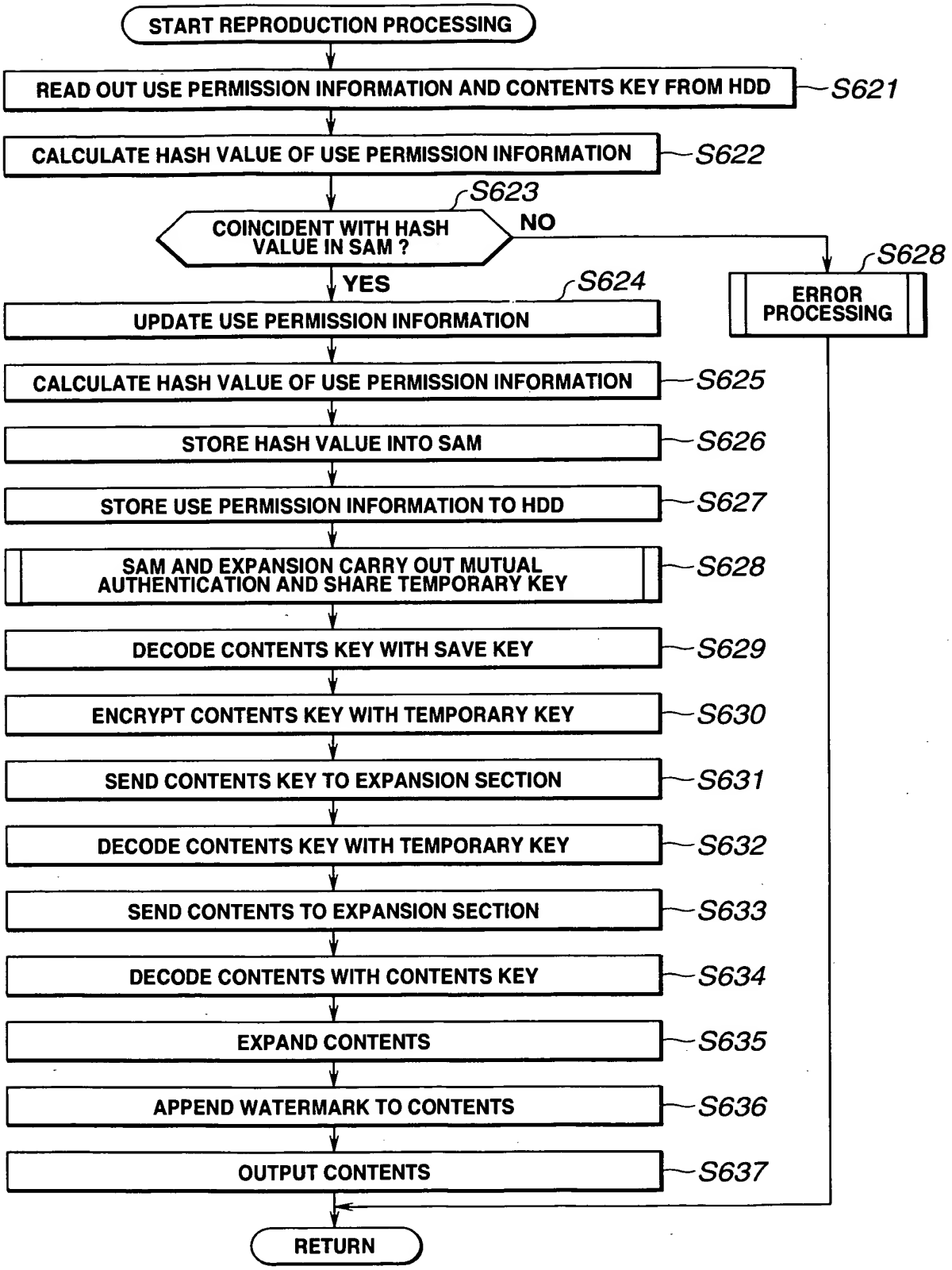
START REPRODUCTION PROCESSING
READ OUT USE PERMISSION INFORMATION AND CONTENTS KEY FROM HDD
S621
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S622
S623
COINCIDENT WITH HASH VALUE IN SAM ?
NO
S628
ERROR PROCESSING
YES
S624
UPDATE USE PERMISSION INFORMATION
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S625
STORE HASH VALUE INTO SAM
S626
STORE USE PERMISSION INFORMATION TO HDD
S627
SAM AND EXPANSION CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S628
DECODE CONTENTS KEY WITH SAVE KEY
S629
ENCRYPT CONTENTS KEY WITH TEMPORARY KEY
S630
SEND CONTENTS KEY TO EXPANSION SECTION
S631
DECODE CONTENTS KEY WITH TEMPORARY KEY
S632
SEND CONTENTS TO EXPANSION SECTION
S633
DECODE CONTENTS WITH CONTENTS KEY
S634
EXPAND CONTENTS
S635
APPEND WATERMARK TO CONTENTS
S636
OUTPUT CONTENTS
S637
RETURN

FIG.78

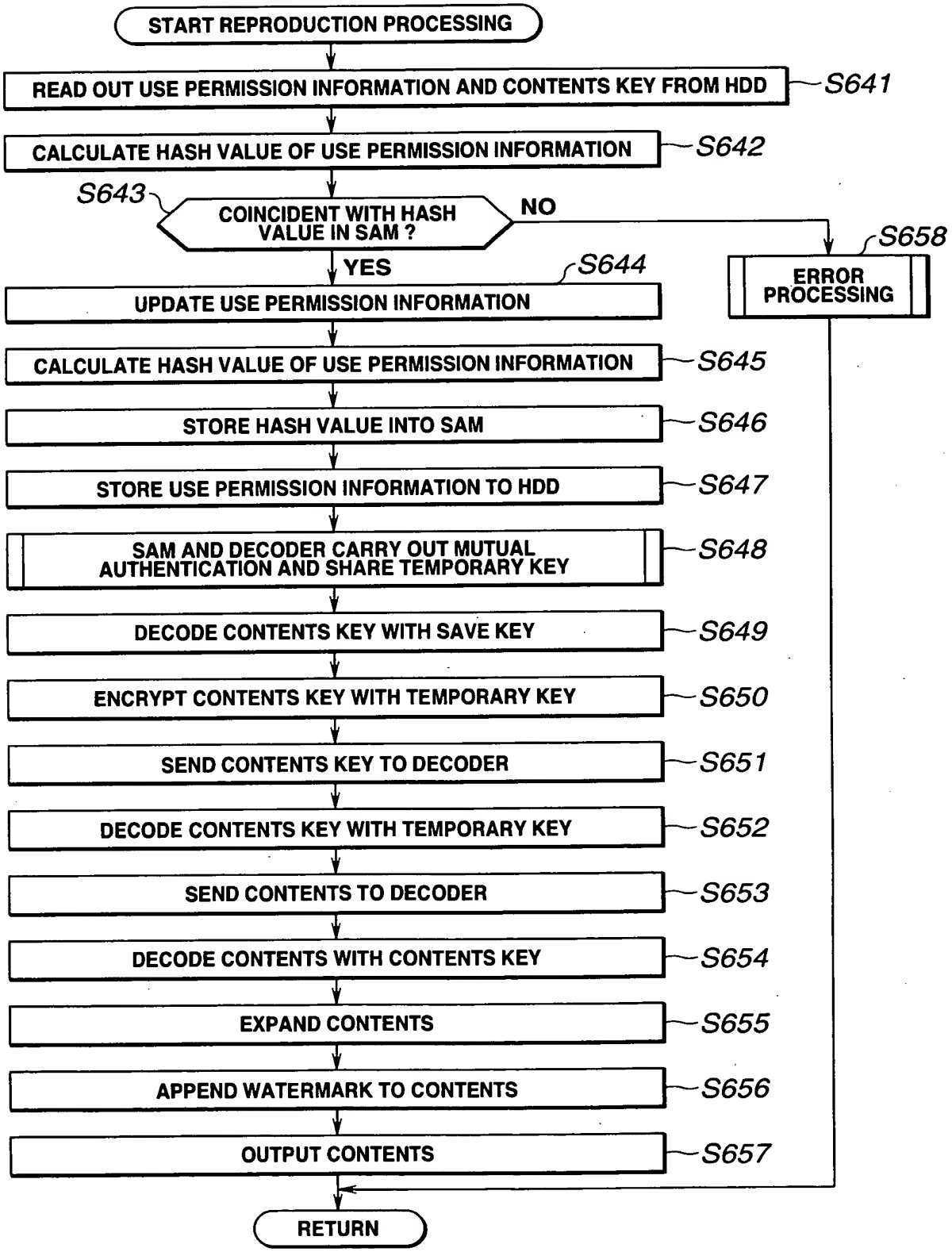
START REPRODUCTION PROCESSING
READ OUT USE PERMISSION INFORMATION AND CONTENTS KEY FROM HDD
S641
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S642
S643
COINCIDENT WITH HASH VALUE IN SAM ?
NO
S658
ERROR PROCESSING
YES
S644
UPDATE USE PERMISSION INFORMATION
CALCULATE HASH VALUE OF USE PERMISSION INFORMATION
S645
STORE HASH VALUE INTO SAM
S646
STORE USE PERMISSION INFORMATION TO HDD
S647
SAM AND DECODER CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S648
DECODE CONTENTS KEY WITH SAVE KEY
S649
ENCRYPT CONTENTS KEY WITH TEMPORARY KEY
S650
SEND CONTENTS KEY TO DECODER
S651
DECODE CONTENTS KEY WITH TEMPORARY KEY
S652
SEND CONTENTS TO DECODER
S653
DECODE CONTENTS WITH CONTENTS KEY
S654
EXPAND CONTENTS
S655
APPEND WATERMARK TO CONTENTS
S656
OUTPUT CONTENTS
S657
RETURN

FIG.79

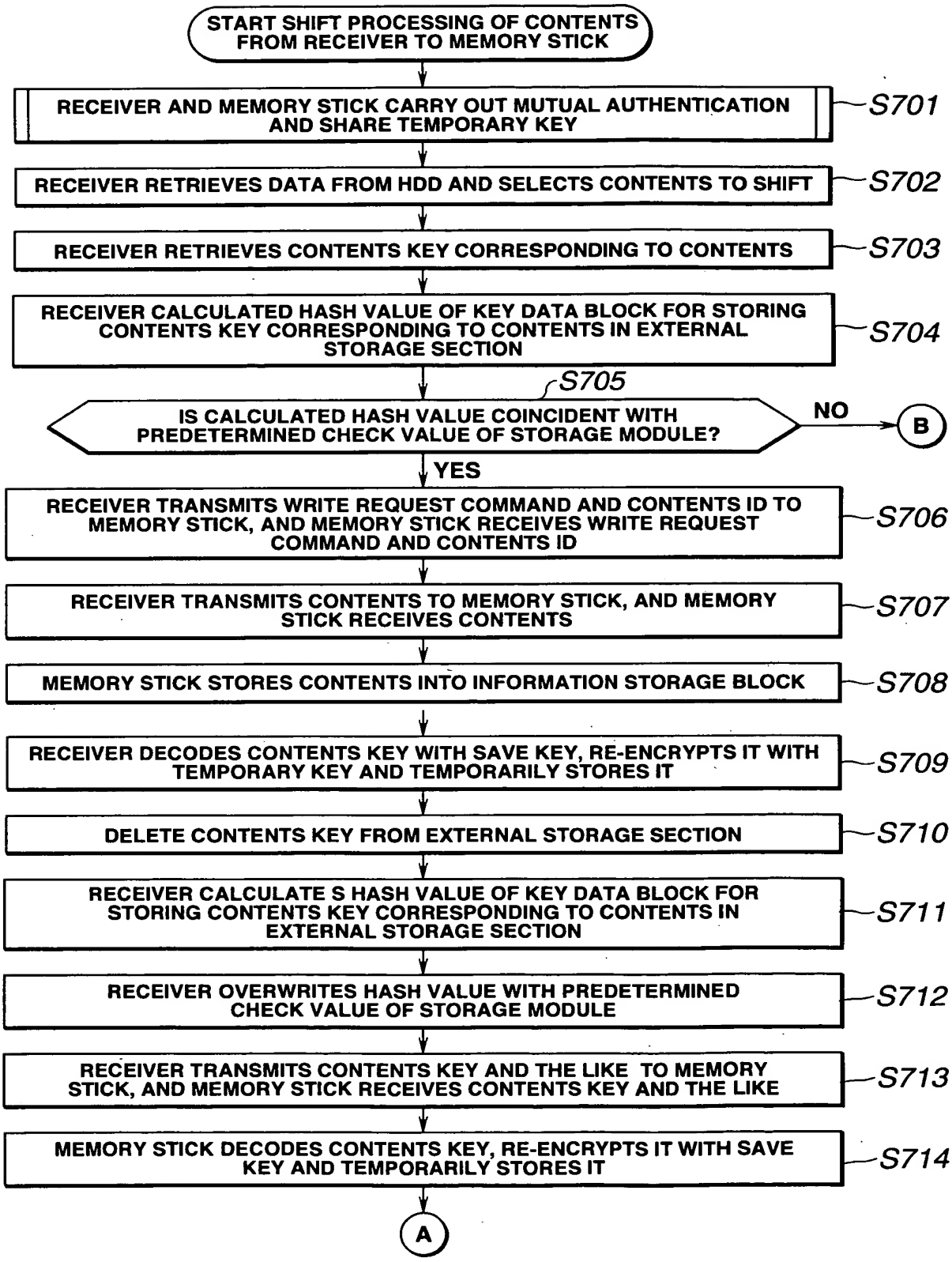
START SHIFT PROCESSING OF CONTENTS FROM RECEIVER TO MEMORY STICK
RECEIVER AND MEMORY STICK CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S701
RECEIVER RETRIEVES DATA FROM HDD AND SELECTS CONTENTS TO SHIFT
S702
RECEIVER RETRIEVES CONTENTS KEY CORRESPONDING TO CONTENTS
S703
RECEIVER CALCULATED HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS IN EXTERNAL STORAGE SECTION
S704
S705
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE?
NO
B
YES
RECEIVER TRANSMITS WRITE REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES WRITE REQUEST COMMAND AND CONTENTS ID
S706
RECEIVER TRANSMITS CONTENTS TO MEMORY STICK, AND MEMORY STICK RECEIVES CONTENTS
S707
MEMORY STICK STORES CONTENTS INTO INFORMATION STORAGE BLOCK
S708
RECEIVER DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND TEMPORARILY STORES IT
S709
DELETE CONTENTS KEY FROM EXTERNAL STORAGE SECTION
S710
RECEIVER CALCULATE S HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS IN EXTERNAL STORAGE SECTION
S711
RECEIVER OVERWRITES HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE
S712
RECEIVER TRANSMITS CONTENTS KEY AND THE LIKE TO MEMORY STICK, AND MEMORY STICK RECEIVES CONTENTS KEY AND THE LIKE
S713
MEMORY STICK DECODES CONTENTS KEY, RE-ENCRYPTS IT WITH SAVE KEY AND TEMPORARILY STORES IT
S714
A

FIG.80

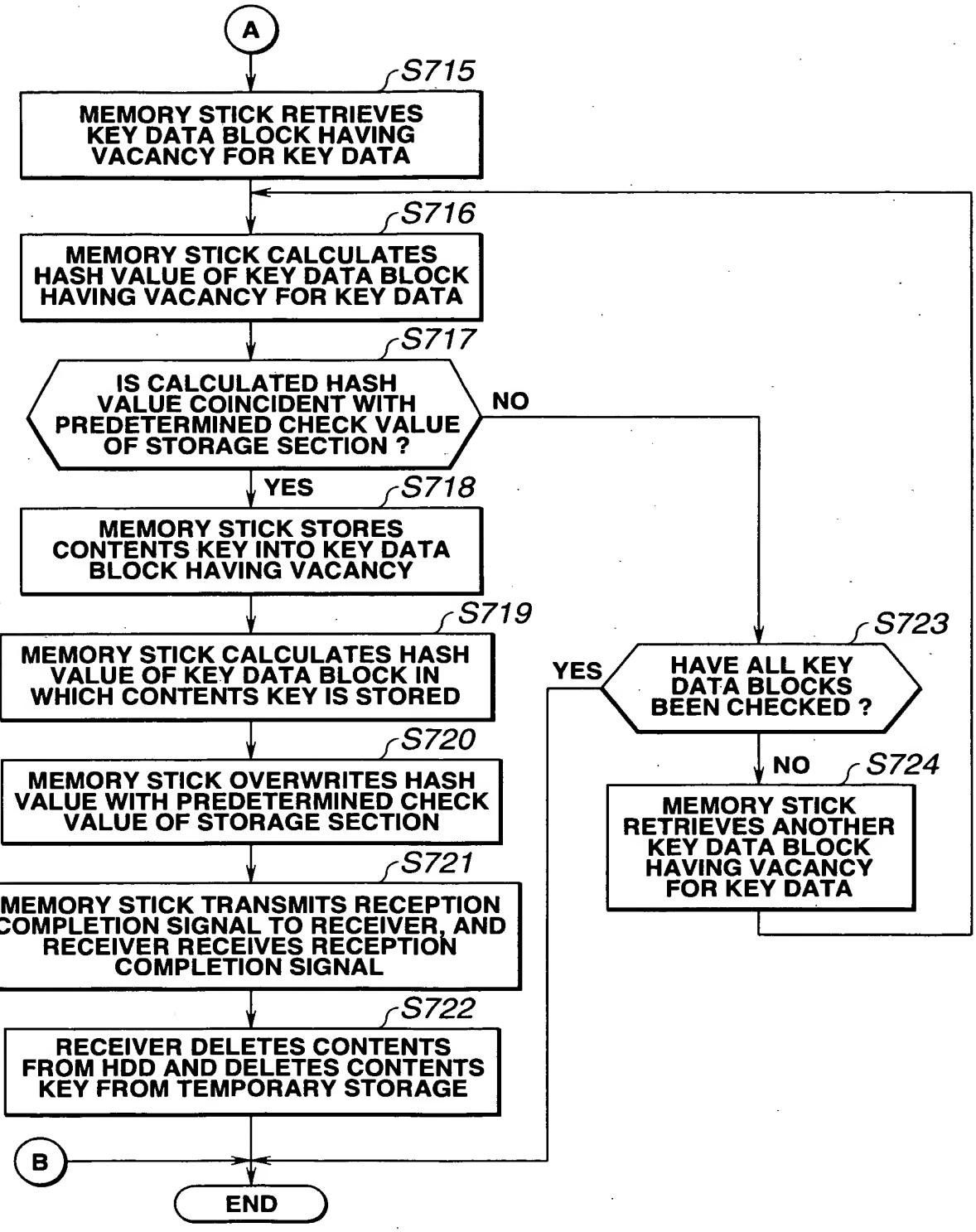
A
S715
MEMORY STICK RETRIEVES KEY DATA BLOCK HAVING VACANCY FOR KEY DATA
S716
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK HAVING VACANCY FOR KEY DATA
S717
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE SECTION ?
NO
YES
S718
MEMORY STICK STORES CONTENTS KEY INTO KEY DATA BLOCK HAVING VACANCY
S719
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK IN WHICH CONTENTS KEY IS STORED
S720
MEMORY STICK OVERWRITES HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE SECTION
S721
MEMORY STICK TRANSMITS RECEPTION COMPLETION SIGNAL TO RECEIVER, AND RECEIVER RECEIVES RECEPTION COMPLETION SIGNAL
S722
RECEIVER DELETES CONTENTS FROM HDD AND DELETES CONTENTS KEY FROM TEMPORARY STORAGE
B
END
S723
YES
HAVE ALL KEY DATA BLOCKS BEEN CHECKED ?
NO
S724
MEMORY STICK RETRIEVES ANOTHER KEY DATA BLOCK HAVING VACANCY FOR KEY DATA

FIG.81

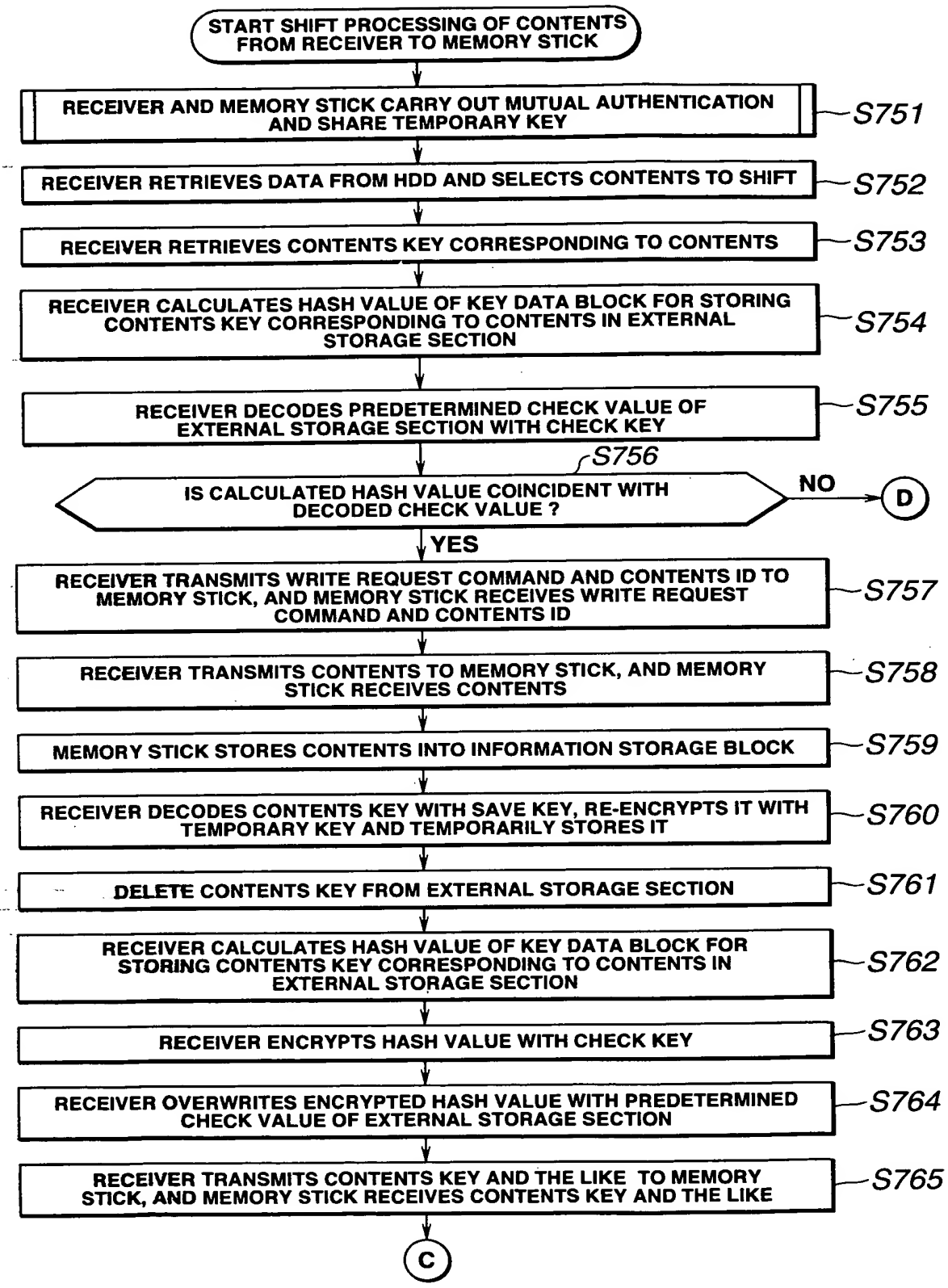

FIG.82

09/581583 - 05/15/2006

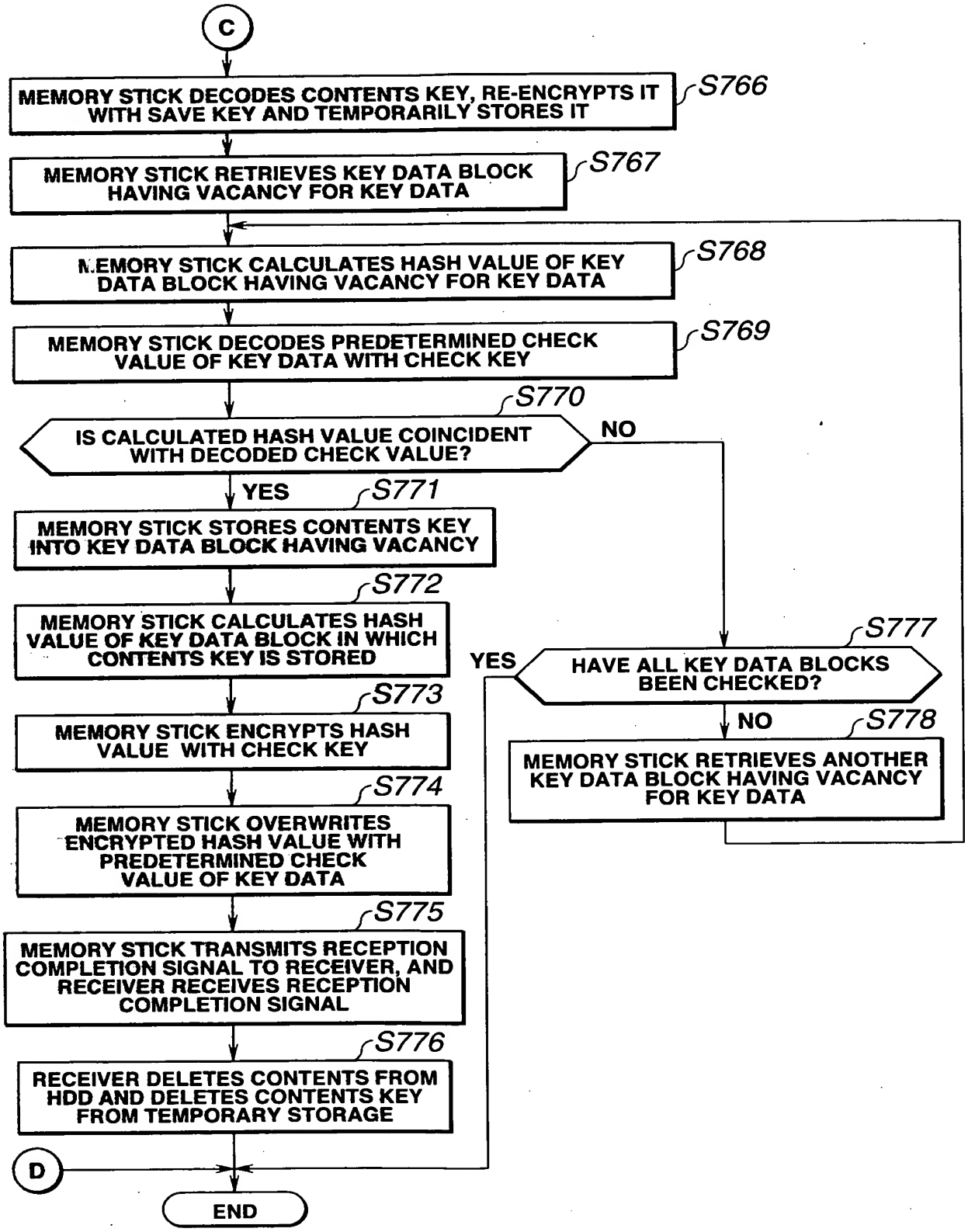
C
MEMORY STICK DECODES CONTENTS KEY, RE-ENCRYPTS IT WITH SAVE KEY AND TEMPORARILY STORES IT
S766
MEMORY STICK RETRIEVES KEY DATA BLOCK HAVING VACANCY FOR KEY DATA
S767
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK HAVING VACANCY FOR KEY DATA
S768
MEMORY STICK DECODES PREDETERMINED CHECK VALUE OF KEY DATA WITH CHECK KEY
S769
S770
IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE?
NO
YES
S771
MEMORY STICK STORES CONTENTS KEY INTO KEY DATA BLOCK HAVING VACANCY
S772
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK IN WHICH CONTENTS KEY IS STORED
S773
MEMORY STICK ENCRYPTS HASH VALUE WITH CHECK KEY
S774
MEMORY STICK OVERWRITES ENCRYPTED HASH VALUE WITH PREDETERMINED CHECK VALUE OF KEY DATA
S775
MEMORY STICK TRANSMITS RECEPTION COMPLETION SIGNAL TO RECEIVER, AND RECEIVER RECEIVES RECEPTION COMPLETION SIGNAL
S776
RECEIVER DELETES CONTENTS FROM HDD AND DELETES CONTENTS KEY FROM TEMPORARY STORAGE
D
END
S777
YES
HAVE ALL KEY DATA BLOCKS BEEN CHECKED?
NO
S778
MEMORY STICK RETRIEVES ANOTHER KEY DATA BLOCK HAVING VACANCY FOR KEY DATA

FIG.83

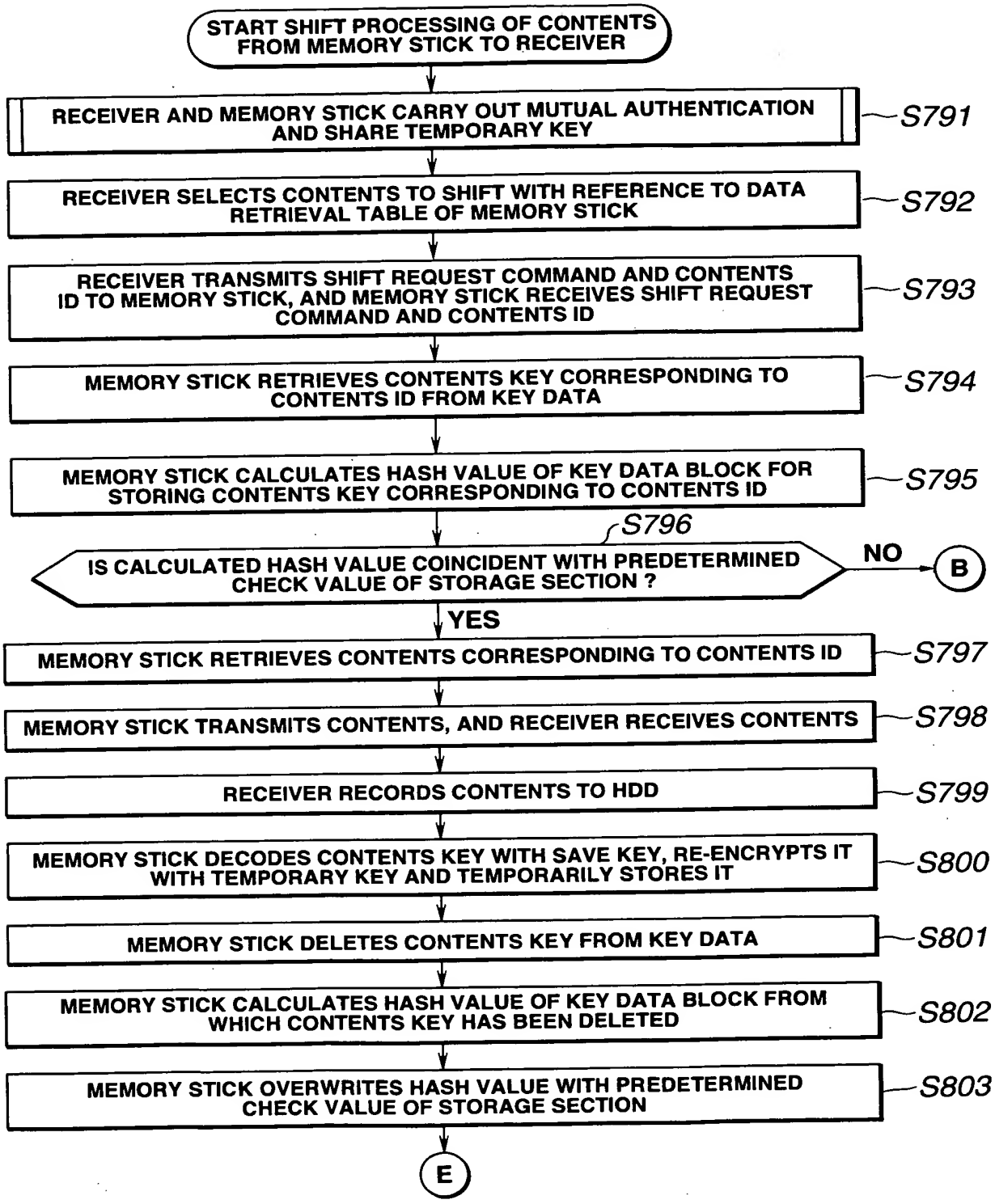
START SHIFT PROCESSING OF CONTENTS FROM MEMORY STICK TO RECEIVER
RECEIVER AND MEMORY STICK CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S791
RECEIVER SELECTS CONTENTS TO SHIFT WITH REFERENCE TO DATA RETRIEVAL TABLE OF MEMORY STICK
S792
RECEIVER TRANSMITS SHIFT REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES SHIFT REQUEST COMMAND AND CONTENTS ID
S793
MEMORY STICK RETRIEVES CONTENTS KEY CORRESPONDING TO CONTENTS ID FROM KEY DATA
S794
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS ID
S795
S796
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE SECTION ?
NO
B
YES
MEMORY STICK RETRIEVES CONTENTS CORRESPONDING TO CONTENTS ID
S797
MEMORY STICK TRANSMITS CONTENTS, AND RECEIVER RECEIVES CONTENTS
S798
RECEIVER RECORDS CONTENTS TO HDD
S799
MEMORY STICK DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND TEMPORARILY STORES IT
S800
MEMORY STICK DELETES CONTENTS KEY FROM KEY DATA
S801
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FROM WHICH CONTENTS KEY HAS BEEN DELETED
S802
MEMORY STICK OVERWRITES HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE SECTION
S803
E

FIG.84

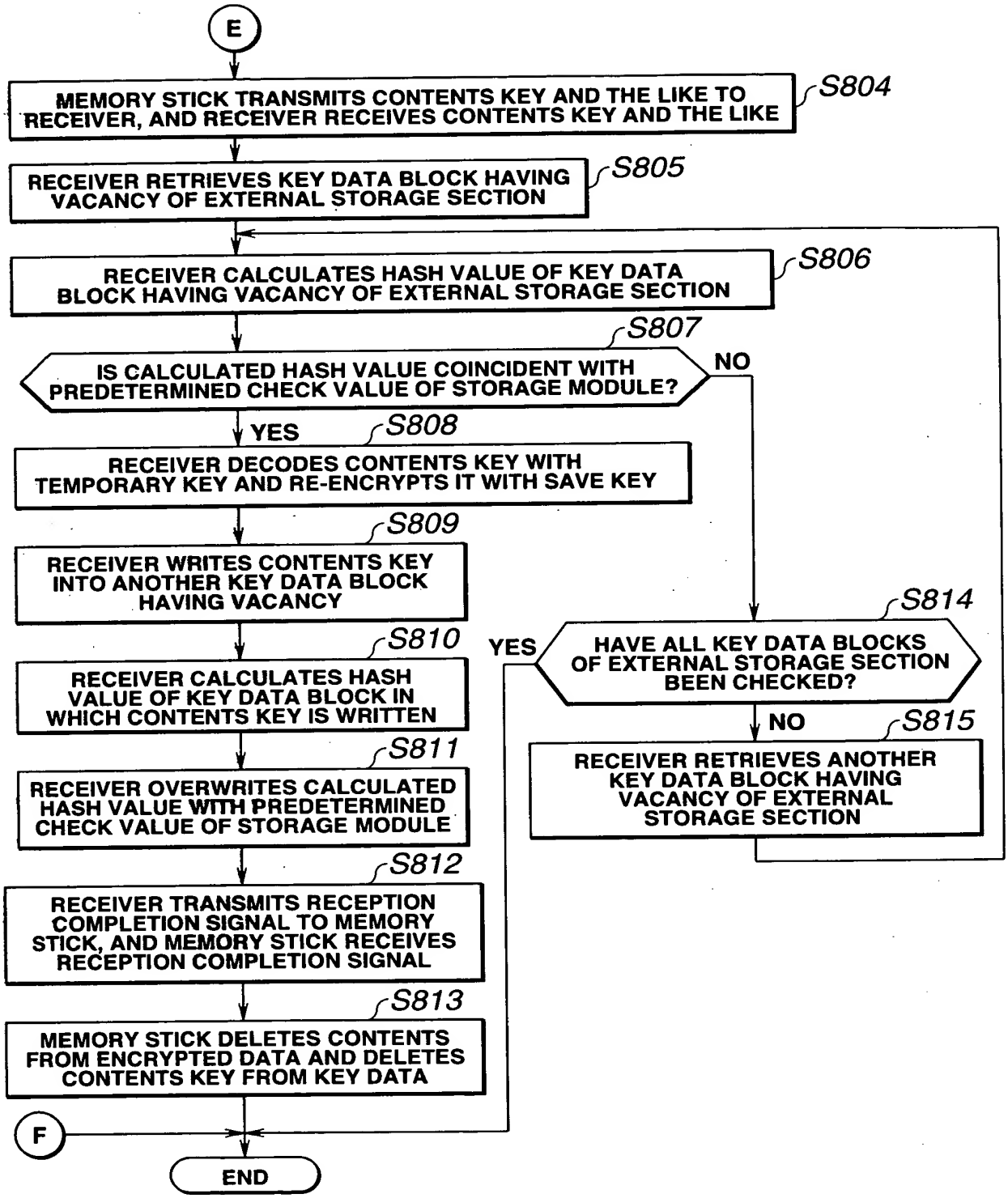
E
MEMORY STICK TRANSMITS CONTENTS KEY AND THE LIKE TO RECEIVER, AND RECEIVER RECEIVES CONTENTS KEY AND THE LIKE
S804
RECEIVER RETRIEVES KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S805
RECEIVER CALCULATES HASH VALUE OF KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S806
S807
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE?
NO
YES
S808
RECEIVER DECODES CONTENTS KEY WITH TEMPORARY KEY AND RE-ENCRYPTS IT WITH SAVE KEY
S809
RECEIVER WRITES CONTENTS KEY INTO ANOTHER KEY DATA BLOCK HAVING VACANCY
S810
RECEIVER CALCULATES HASH VALUE OF KEY DATA BLOCK IN WHICH CONTENTS KEY IS WRITTEN
S811
RECEIVER OVERWRITES CALCULATED HASH VALUE WITH PREDETERMINED CHECK VALUE OF STORAGE MODULE
S812
RECEIVER TRANSMITS RECEPTION COMPLETION SIGNAL TO MEMORY STICK, AND MEMORY STICK RECEIVES RECEPTION COMPLETION SIGNAL
S813
MEMORY STICK DELETES CONTENTS FROM ENCRYPTED DATA AND DELETES CONTENTS KEY FROM KEY DATA
F
END
S814
YES
HAVE ALL KEY DATA BLOCKS OF EXTERNAL STORAGE SECTION BEEN CHECKED?
NO
S815
RECEIVER RETRIEVES ANOTHER KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION

FIG.85

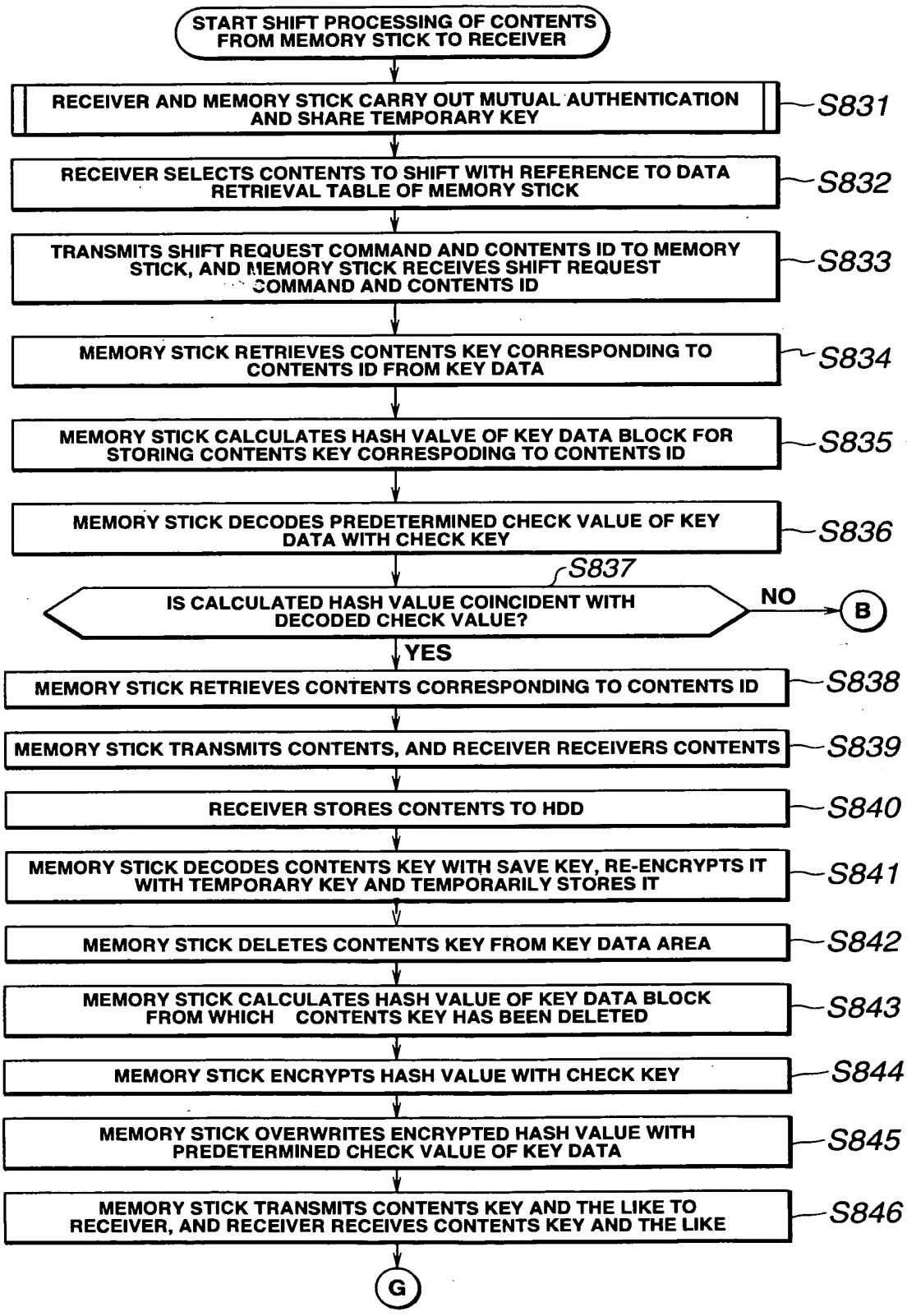
START SHIFT PROCESSING OF CONTENTS FROM MEMORY STICK TO RECEIVER
RECEIVER AND MEMORY STICK CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S831
RECEIVER SELECTS CONTENTS TO SHIFT WITH REFERENCE TO DATA RETRIEVAL TABLE OF MEMORY STICK
S832
TRANSMITS SHIFT REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES SHIFT REQUEST COMMAND AND CONTENTS ID
S833
MEMORY STICK RETRIEVES CONTENTS KEY CORRESPONDING TO CONTENTS ID FROM KEY DATA
S834
MEMORY STICK CALCULATES HASH VALVE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPODING TO CONTENTS ID
S835
MEMORY STICK DECODES PREDETERMINED CHECK VALUE OF KEY DATA WITH CHECK KEY
S836
S837
IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE?
NO
B
YES
MEMORY STICK RETRIEVES CONTENTS CORRESPONDING TO CONTENTS ID
S838
MEMORY STICK TRANSMITS CONTENTS, AND RECEIVER RECEIVERS CONTENTS
S839
RECEIVER STORES CONTENTS TO HDD
S840
MEMORY STICK DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND TEMPORARILY STORES IT
S841
MEMORY STICK DELETES CONTENTS KEY FROM KEY DATA AREA
S842
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FROM WHICH CONTENTS KEY HAS BEEN DELETED
S843
MEMORY STICK ENCRYPTS HASH VALUE WITH CHECK KEY
S844
MEMORY STICK OVERWRITES ENCRYPTED HASH VALUE WITH PREDETERMINED CHECK VALUE OF KEY DATA
S845
MEMORY STICK TRANSMITS CONTENTS KEY AND THE LIKE TO RECEIVER, AND RECEIVER RECEIVES CONTENTS KEY AND THE LIKE
S846
G

FIG.86

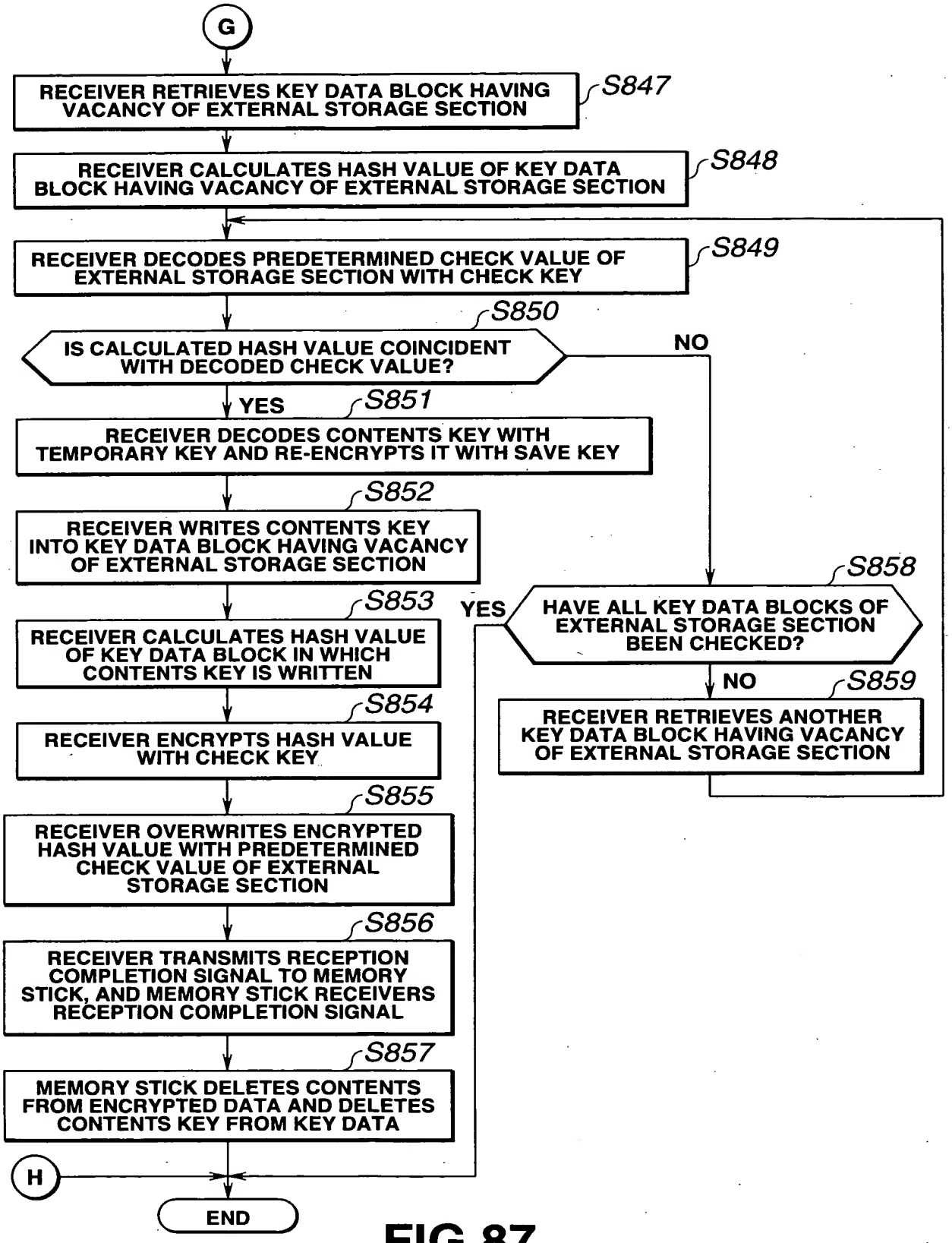
G
RECEIVER RETRIEVES KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S847
RECEIVER CALCULATES HASH VALUE OF KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S848
RECEIVER DECODES PREDETERMINED CHECK VALUE OF EXTERNAL STORAGE SECTION WITH CHECK KEY
S849
S850
IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE?
NO
YES
S851
RECEIVER DECODES CONTENTS KEY WITH TEMPORARY KEY AND RE-ENCRYPTS IT WITH SAVE KEY
S852
RECEIVER WRITES CONTENTS KEY INTO KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION
S853
RECEIVER CALCULATES HASH VALUE OF KEY DATA BLOCK IN WHICH CONTENTS KEY IS WRITTEN
S854
RECEIVER ENCRYPTS HASH VALUE WITH CHECK KEY
S855
RECEIVER OVERWRITES ENCRYPTED HASH VALUE WITH PREDETERMINED CHECK VALUE OF EXTERNAL STORAGE SECTION
S856
RECEIVER TRANSMITS RECEPTION COMPLETION SIGNAL TO MEMORY STICK, AND MEMORY STICK RECEIVERS RECEPTION COMPLETION SIGNAL
S857
MEMORY STICK DELETES CONTENTS FROM ENCRYPTED DATA AND DELETES CONTENTS KEY FROM KEY DATA
H
END
S858
YES
HAVE ALL KEY DATA BLOCKS OF EXTERNAL STORAGE SECTION BEEN CHECKED?
NO
S859
RECEIVER RETRIEVES ANOTHER KEY DATA BLOCK HAVING VACANCY OF EXTERNAL STORAGE SECTION

FIG.87

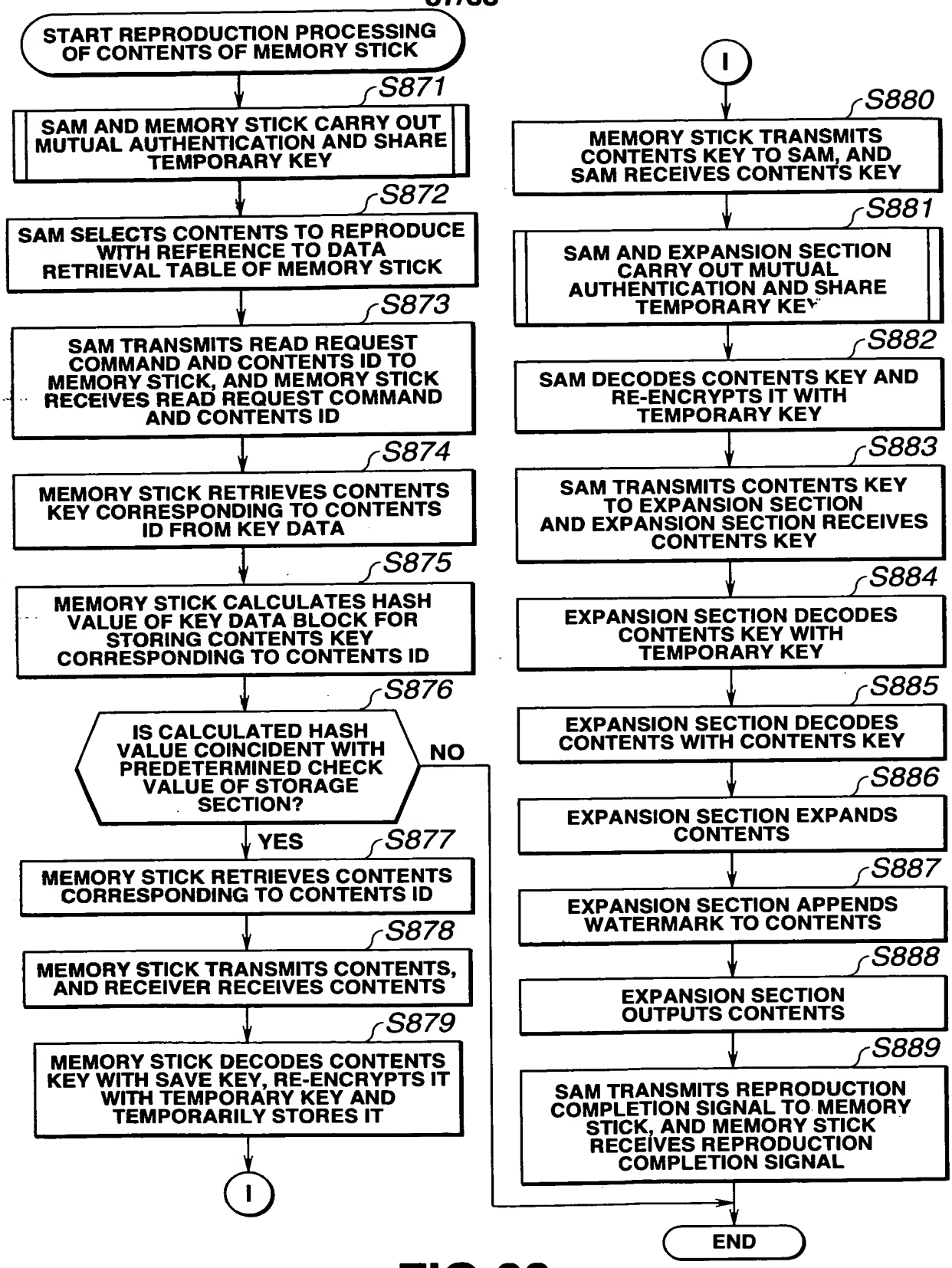
START REPRODUCTION PROCESSING OF CONTENTS OF MEMORY STICK
S871
SAM AND MEMORY STICK CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S872
SAM SELECTS CONTENTS TO REPRODUCE WITH REFERENCE TO DATA RETRIEVAL TABLE OF MEMORY STICK
S873
SAM TRANSMITS READ REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES READ REQUEST COMMAND AND CONTENTS ID
S874
MEMORY STICK RETRIEVES CONTENTS KEY CORRESPONDING TO CONTENTS ID FROM KEY DATA
S875
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS ID
S876
IS CALCULATED HASH VALUE COINCIDENT WITH PREDETERMINED CHECK VALUE OF STORAGE SECTION?
NO
YES
S877
MEMORY STICK RETRIEVES CONTENTS CORRESPONDING TO CONTENTS ID
S878
MEMORY STICK TRANSMITS CONTENTS, AND RECEIVER RECEIVES CONTENTS
S879
MEMORY STICK DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND TEMPORARILY STORES IT
I
I
S880
MEMORY STICK TRANSMITS CONTENTS KEY TO SAM, AND SAM RECEIVES CONTENTS KEY
S881
SAM AND EXPANSION SECTION CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S882
SAM DECODES CONTENTS KEY AND RE-ENCRYPTS IT WITH TEMPORARY KEY
S883
SAM TRANSMITS CONTENTS KEY TO EXPANSION SECTION AND EXPANSION SECTION RECEIVES CONTENTS KEY
S884
EXPANSION SECTION DECODES CONTENTS KEY WITH TEMPORARY KEY
S885
EXPANSION SECTION DECODES CONTENTS WITH CONTENTS KEY
S886
EXPANSION SECTION EXPANDS CONTENTS
S887
EXPANSION SECTION APPENDS WATERMARK TO CONTENTS
S888
EXPANSION SECTION OUTPUTS CONTENTS
S889
SAM TRANSMITS REPRODUCTION COMPLETION SIGNAL TO MEMORY STICK, AND MEMORY STICK RECEIVES REPRODUCTION COMPLETION SIGNAL
END

FIG.88

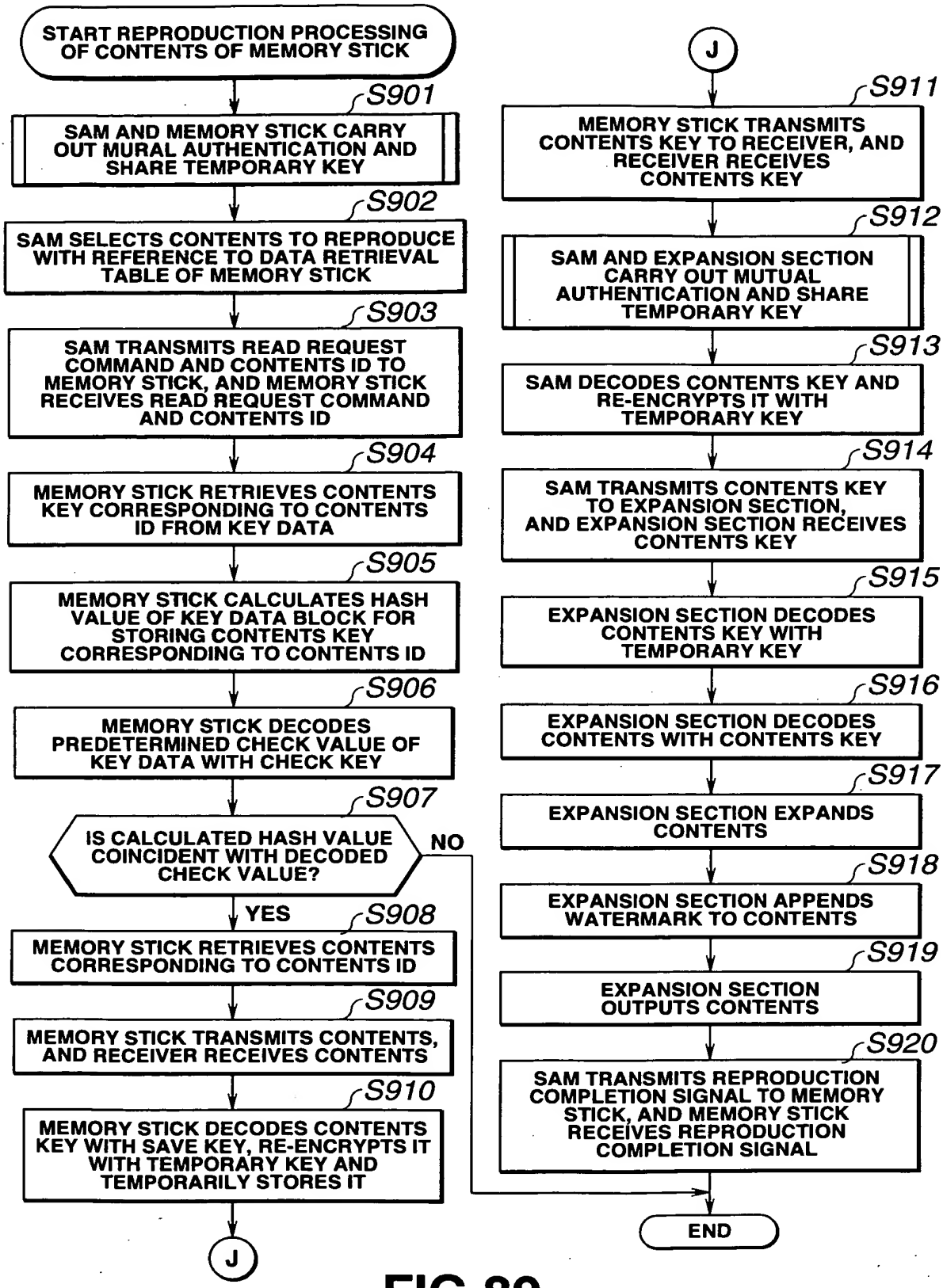
START REPRODUCTION PROCESSING OF CONTENTS OF MEMORY STICK
S901
SAM AND MEMORY STICK CARRY OUT MURAL AUTHENTICATION AND SHARE TEMPORARY KEY
S902
SAM SELECTS CONTENTS TO REPRODUCE WITH REFERENCE TO DATA RETRIEVAL TABLE OF MEMORY STICK
S903
SAM TRANSMITS READ REQUEST COMMAND AND CONTENTS ID TO MEMORY STICK, AND MEMORY STICK RECEIVES READ REQUEST COMMAND AND CONTENTS ID
S904
MEMORY STICK RETRIEVES CONTENTS KEY CORRESPONDING TO CONTENTS ID FROM KEY DATA
S905
MEMORY STICK CALCULATES HASH VALUE OF KEY DATA BLOCK FOR STORING CONTENTS KEY CORRESPONDING TO CONTENTS ID
S906
MEMORY STICK DECODES PREDETERMINED CHECK VALUE OF KEY DATA WITH CHECK KEY
S907
IS CALCULATED HASH VALUE COINCIDENT WITH DECODED CHECK VALUE?
NO
YES
S908
MEMORY STICK RETRIEVES CONTENTS CORRESPONDING TO CONTENTS ID
S909
MEMORY STICK TRANSMITS CONTENTS, AND RECEIVER RECEIVES CONTENTS
S910
MEMORY STICK DECODES CONTENTS KEY WITH SAVE KEY, RE-ENCRYPTS IT WITH TEMPORARY KEY AND TEMPORARILY STORES IT
J
J
S911
MEMORY STICK TRANSMITS CONTENTS KEY TO RECEIVER, AND RECEIVER RECEIVES CONTENTS KEY
S912
SAM AND EXPANSION SECTION CARRY OUT MUTUAL AUTHENTICATION AND SHARE TEMPORARY KEY
S913
SAM DECODES CONTENTS KEY AND RE-ENCRYPTS IT WITH TEMPORARY KEY
S914
SAM TRANSMITS CONTENTS KEY TO EXPANSION SECTION, AND EXPANSION SECTION RECEIVES CONTENTS KEY
S915
EXPANSION SECTION DECODES CONTENTS KEY WITH TEMPORARY KEY
S916
EXPANSION SECTION DECODES CONTENTS WITH CONTENTS KEY
S917
EXPANSION SECTION EXPANDS CONTENTS
S918
EXPANSION SECTION APPENDS WATERMARK TO CONTENTS
S919
EXPANSION SECTION OUTPUTS CONTENTS
S920
SAM TRANSMITS REPRODUCTION COMPLETION SIGNAL TO MEMORY STICK, AND MEMORY STICK RECEIVES REPRODUCTION COMPLETION SIGNAL
END

FIG.89